Volume 1 Number 3 August 2015

The Army War College Review

Student Publications

UNITED STATES ARMY WAR COLLEGE PRESS
Carlisle Barracks, PA
STRENGTH and WISDOM

The Army War College Review

The Army War College Review, a refereed publication of student work, is produced under the purview of the Strategic Studies Institute and the United States Army War College. An electronic quarterly, *The AWC Review* connects student intellectual work with professionals invested in U.S. national security, Landpower, strategic leadership, global security studies, and the advancement of the profession of arms.

The Army War College Review
Larry D. Miller, Editor
Student Publications
Root Hall, B-14
Carlisle Barracks, PA 17013-5010
http://www.strategicstudiesinstitute.army.mil/pubs/AWCreview

Design and production courtesy the Institute for Military Writing.

Selection Process

Research articles are selected from among award-winning student papers evaluated by the USAWC Distinguished Academic Chairs as outstanding exemplars of student writing or research at the professional graduate level. *Insight* articles are written primarily by USAWC Fellows, studying off-site at prestigious institutions. The Student Awards Competition is open to all enrolled Resident Students, Distance Education Students, and AWC Fellows. Articles edited for economy and clarity.

USAWC Distinguished Academic Chairs

R. Craig Bullis	Michael A. Marra	Jerome T. Sibayan
Antulio J. Echevarria II	Michael S. Neiberg	Harry A. Tomlin
Edward J. Filiberti	John J. Patterson VI	Tarn D. Warren
Larry P. Goodson	Thomas E. Sheperd	Leonard Wong
Paul C. Jussel		

Cover

Flag flying over the Strength and Wisdom statue, a gift from the class of 2014, capturing the mission, spirit, and history of Carlisle Barracks (photo by Laura A. Wackwitz, Ph.D.).

Disclaimer

The United States Army War College
Student Publications

The Army War College Review

Volume 1 ▪ Number 3 ▪ August 2015

Research

Insights

Army War College Review
Vol. 1, No. 3, Aug. 2015, 1-12

U.S. Army War College
Student Publications

Laws of Unintended Consequences: The Leahy Laws

Tim L. Rieger

The United States remains in a global war on terror and faces clear and present security threats in every region of the world. At the same time, the U.S. is committed as a matter of national strategic policy to protecting human rights and advancing the rule of law throughout the world. To achieve regional security the United States must cooperate with, train and assist foreign military units, or individuals, accused of violating human rights. In order to reconcile these conflicting requirements, promote accountability and military competence for national security at the strategic level, advance the rule of law at the international level, and protect human rights; U.S. law should be amended. All U.S. military training and assistance by Special Operations Forces, Legal Officers, and Commanders with experience in Rule of Law and Human Rights Operations should be authorized to train foreign military units accused of gross violations of human rights.

Keywords: *Special Forces Operations, Human Rights, Military Training Assistance, Coalitions*

> We must all hang together, or assuredly we shall all hang separately.
>
> —Benjamin Franklin[1]

The United States is committed as a matter of national strategic policy to protecting human rights and advancing the rule of law throughout the world. At the same time, the U.S. continues to fight a global war on terror and face security threats in every region of the world. The U.S. works with, and relies heavily upon, regional partners to combat terrorism, ensure regional security, and promote the global commons for trade. Achieving multi-lateral political stability and international prosperity often requires cooperation, training and assistance with foreign military units and individuals accused of committing gross violations of human rights. A plethora of human rights laws embedded in many different acts of Congress arguably limit the ability of the executive to engage in unfettered

---

Tim L. Rieger (M.S.S. United States Army War College) is a Colonel in the United States Army National Guard. *An earlier version of this article, written under the direction of Professor Paul C. Jussel, earned a prestigious U.S. Military Academy William E. Simon Center for Professional Military Ethic Writing Award for the USAWC class of 2015.*

[1] Benjamin Franklin, *Declaration of Independence*, Philadelphia, PA. Statement attributed as Franklin signed the United States Declaration of Independence from Great Britain, July 4, 1776, linked from the *Historic Valley Forge Website* http://www.ushistory.org/valleyforge/history/franklin.html (accessed February 26, 2015).

foreign relations.[2] Most of these limitations restrict the expenditure of funds to support foreign economies, political entities, military, security forces, and police agencies.

Currently, the Leahy Laws, for example, prohibit the U.S. from providing foreign assistance, military assistance, and military training to foreign units or individuals accused of gross violations of human rights.[3] Such allegations and accusations could be, and have been, made against individuals and units in the United States military and government, as well. In fact, allegations against U.S. personnel are among the reasons the United States has yet to participate in the Rome Treaty and the International Criminal Court system.[4] A balance must be reached between the need for accountability and military competence of U.S. regional partners. In order to assist in reconciling seemingly competing interests, the Leahy Laws should be amended to authorize U.S. military training and assistance to foreign military units accused of gross violations of human rights in the Law of Armed Conflict, the Code of Conduct, Human Rights, Military Justice, and the ramifications of International Criminal Justice.

The unintended consequences of the Leahy Laws are that the very allies that need the most training in rule of law, rules of engagement, rules for the use of force, law of armed conflict, military justice, and command and control of troops are prohibited from receiving that training from U.S. advisors and military personnel. Denial of opportunity creates a vacuum sometimes filled by other nations where a partnership with the U.S. military would better serve all concerned. Ironically, and perhaps most importantly, because of the lack of training with U.S. forces, human rights arguably receive less emphasis and are more likely to be violated by the very military units that most need—but are denied—U.S. military training and assistance.

In order to promote national security at the strategic level, the rule of law at the international level, and to protect international human rights, the U.S. must (a) clarify definitions of elements of the Leahy Laws, (b) provide adequate funding for vetting and human rights programs, (c) ensure greater training about the Leahy Laws in the U.S. Department of State (DoS) and the U.S. Department of Defense (DoD), and most importantly, (d) the U.S. should assist in the training and promotion of human rights with international military and government partners. The Leahy Laws should be amended to authorize qualified U.S. forces with experience in Rule of Law and Humanitarian Assistance Operations to train foreign military units accused of gross violations of human rights.

The Competing United States Strategic Interests

Tension exists between the promotion of human rights and the need to work with coalition partner military and security forces. One of the principal methods of international security cooperation is training, equipping, and assisting foreign militaries. As noted by former Secretary of Defense Hagel, “In many regions we are witnessing the emergence of international partners with the

---

[2] An overview of United States Human Rights policy, law, and implementation is available from the United States Department of State. See *Diplomacy in Action*, *Human Rights Online*, http://www.state.gov/j/drl/hr/ (accessed February 24, 2015).

[3] Ibid. See also, *University of Minnesota Human Rights bibliography of United States Human Rights Legislation*, http://www1.umn.edu/humanrts/demo/biblio.htm#r1 (accessed January 21, 2015).

[4] Keith Pesto, Judge, “The International Criminal Court: An Opposing View,” *Juniata College Press Online*, (April 27, 2012) http://www.juniata.edu/services/jcpress/voices/pdf/2012/jv_2012_139-144.pdf (accessed February 4, 2015). See also, Matthew Gulger, “The International Criminal Court: Why is the United States not a Member?” *The American Humanist Online*, (2013) http://americanhumanist.org/HNN/details/2013-06-the-international-criminal-court-why-is-the-united-s (accessed February 15, 2015).

capacity to play productive and even leading security roles in their respective regions."[5] Additional military training and assistance in these regions is the primary method ("way") to achieve greater regional stability and strengthen alignments with U.S. strategic goals. In Asia, Former Secretary Hagel specifically articulated the importance of several nations as "traditional anchors" of regional partnership and evolving security, but both South Korea and Indonesia have had significant issues with allegations of human rights abuses in the past. [6] In Africa, the emphasis on stability from the U.S.'s perspective is the "significant opportunity to develop stronger governance institutions and to help build professional, capable military forces that can partner with the United States to address the full spectrum of regional security challenges." [7] African partnerships can be particularly problematic from the human rights vetting perspective. Allegations, for example, against Nigerian military units and members in their fight against the Islamic terrorist organization Boko Haram have proven difficult to vet. Former Secretary Hagel noted that "The United States is willing to undertake security cooperation with Russia, both in the bilateral context and in seeking solutions to regional challenges . . . ."[8] Russian military activities in Chechnya, Crimea, Georgia, Ukraine, and other areas in recent years could require significant vetting if cooperation extended to security training with the Russian military.

The dichotomy between the competing human rights interests and operations with strategic partners is summarized succinctly in the *2014 Quadrennial Review*.[9] National security and military strategies for cooperation and collaboration with regional partners are essential in an era of reduced resources, shared security costs, and international command and control if strategic objectives are to be achieved. The U.S. Army and DoD must work more closely with allied nations to ensure the Rule of Law in partner nations. In the efforts to promote international humanitarian law, the U.S. must not jeopardize international security, the safety of the American people, nor our relationship with allies and potential allies.

Human rights are an essential aspect of the character of the United States, "Yet obviously," observed National Security Advisor Susan Rice, "advancing human rights is not and has never been our only interest. Every U.S. president has a sworn duty to protect the lives and the fortunes of the American people against immediate threats." She continued by asserting that improperly weighing these interests and failing to act could amount to dereliction of duty, opining:

> We must defend the United States, our citizens and our allies with every tool at our disposal, including, when necessary, with military force. We must do all we can to counter weapons of mass destruction, aggression, terrorism, and catastrophic threats to the global economy, upon which our way of life depends. Anything less would be a dereliction of duty.[10]

---

[5] Chuck Hagel, *Quadrennial Defense Review Online* (Washington, DC: U.S. Department of Defense, March, 4, 2014): 6, http://www.defense.gov/pubs/2014_Quadrennial_Defense_Review.pdf (accessed December 11, 2014).

[6] Ibid., 4.

[7] Ibid., 5.

[8] Ibid., 6.

[9] In pertinent part states, "Built on a foundation of common interests and shared values, the strength of U.S. alliances and partnerships is unparalleled. People around the world gravitate toward the freedom, equality, rule of law, and democratic governance that American citizens are able to enjoy. From setting global norms to defeating terrorist threats and providing humanitarian assistance, the United States collaborates with allies and partners to accomplish a wide range of strategic, operational, and tactical goals. We leverage U.S. leadership and capabilities to drive global cooperation on security challenges in the United Nations and other multilateral fora. In recent years alone, we have cooperated with European allies and partners on operations in Afghanistan and Libya and have joined forces with Asian allies and partners on regional security issues. These and other key networks of alliances and partnerships, many of which are with other leading global military powers, will undergird the ability of the United States to face future crises and contingencies." Ibid., 9.

[10] Susan E. Rice, United States National Security Advisor, Remarks by National Security Advisor "Human Rights: Advancing American Interests and Values," at the Human Rights First Annual Summit, Washington, DC, (December 4,

Rice explained the difficult challenges in determining the paramount consideration in any given situation, stating, "As we seek to secure these core interests, we sometimes face painful dilemmas when the immediate need to defend our national security clashes with our fundamental commitment to democracy and human rights." She also emphasized the importance of candor in order to maintain credibility, admitting, "Let's be honest: at times, as a result, we do business with governments that do not respect the rights we hold most dear. We make tough choices. When rights are violated, we continue to advocate for their protection. But we cannot, and I will not pretend that some short-term tradeoffs do not exist."[11] Finally, she suggested that these competing concerns are reconcilable, and that we must be responsive to both requirements, stating, "Still, over time, we know that our core interests are inseparable from our core values, that our commitment to democracy and human rights roundly reinforces our national security."[12]

While the principles of human rights, generally, and the Leahy Laws, specifically, are admirable and remain at the fore of strategic interests, the U.S. should reevaluate and adjust the manner in which these policies are implemented. The U.S. can work closely to promote human rights, the rule of law and international humanitarian law through training and partnership, rather than rejecting and denying training and assistance to security force partners accused of human rights violations.

The Legal Obligation, Framework and History

International legal obligations, fundamental democratic values, and constitutional principles are a few of the many elements that weigh heavily toward U.S. emphasis on human rights in foreign relations. But perhaps the paramount reason for the U.S. military to keep human rights at the forefront of policy and planning is the law. Notably, the foundation of the laws pertaining to DoS and DoD for foreign assistance, military assistance and sales, is found initially in the *Foreign Assistance Act* "Declaration of Policy." [13]

The historic background and evolution of the human rights laws in the *Foreign Assistance Act* leading to the Leahy Laws is significant, illustrating the contentiousness and distrustful history between the Legislative and Executive Branches regarding the relative importance of human rights concerns in foreign relations. The executive branch has constitutional authority and the mandate to engage in international relations but the legislature funds, or not, these activities and diplomatic entreaties.

Almost from the inception of the 1961 *Foreign Assistance Act*, Congress took umbrage with many of the ways it was implemented. The evolutionary track leading to the present state of the Leahy Laws has a 40 year history of adversarial tension between the executive and legislative branches.[14] Foreign assistance for many oppressive regimes and totalitarian human rights violators led to the enactment of Section 32 of the *Foreign Assistance Act*. Cognizant of the separation of powers in the

---

2013): 6, http://www.whitehouse.gov/the-press-office/2013/12/04/remarks-national-security-advisor-susan-e-rice-human-rights-advancing-am (accessed February 22, 2015).

[11] Ibid.

[12] Ibid.

[13] Section 2304, which states, in pertinent part: a. "Observance of human rights as principal goal of foreign policy; implementation requirements. (1) The United States shall, in accordance with its international obligations as set forth in the Charter of the United Nations and in keeping with the constitutional heritage and traditions of the United States, promote and encourage increased respect for human rights and fundamental freedoms throughout the world without distinction as to race, sex, language, or religion. Accordingly, a principal goal of the foreign policy of the United States shall be to promote the increased observance of internationally recognized human rights by all countries."

[14] Stephen B. Cohen, "Conditioning U.S. Security Assistance on Human Rights Practices," *The American Journal of Int'l Law Online* 76, no.2. (April 1982): 246-279, http://web.stanford.edu/class/ips216/Readings/cohen_82%20(Human%20Rights).pdf (accessed December 11, 2014).

Constitution and the Executive's role in foreign affairs and military matters, Congress inserted cautionary language that the President should deny "military assistance to the government of any foreign country which practices the internment or imprisonment of that country's citizens for political purposes."[15] But the statutory language was merely advisory, stating "It is the sense of Congress that the President should deny . . . . "[16] President Nixon ignored the language. In fact, then Secretary of State Henry Kissinger stated, "I hold the strong view that human rights are not appropriate in a foreign policy context."[17] As a consequence, the House conducted hearings and issued a report finding that "Unfortunately, the prevailing attitude [of the Executive branch] has led the United States into embracing governments which practice torture and unabashedly violate almost every human rights guarantee pronounced by the World Community."[18] The report further found this was a dangerous and shortsighted precedent and declared, "Consideration for human rights in foreign policy is both morally imperative and practically necessary."[19] Finally, the Committee observed that "When charges of serious violations of human rights do occur, the most that the [State] Department is likely to do is make private inquiries and low-keyed appeals to the government concerned."[20]

For Congress and their perspective of human rights in foreign policy, President Ford's administration was no improvement. Testifying before Congress, the Under Secretary of State for Security Assistance stated the administration had not acted on the human rights language in the *Foreign Assistance Act* and that no military sales or military aid had been impacted.[21] DoS argued instead that the statute was poor policy and interfered with Executive branch prerogatives in conducting foreign relations.[22] Congress responded by removing the advisory language and finding that, "Unfortunately, the executive branch response to the existing human rights provision has not been satisfactory."[23] Congress noted, "In fact, increased levels of security assistance were requested for a number of countries where serious human rights problems exist."[24] Congress declared, "Consequently, the [new law] makes it binding that the President include human rights considerations in the process in determining levels and kinds of assistance for recipient countries."[25] President Ford vetoed the amendment and only signed the 1976 *International Security Assistance and Arms Export Act* after the legally binding language was removed.[26]

Congress had a human rights advocate in President Carter, who many times during his presidential bid and subsequent administration emphasized human rights and the U.S. government's

---

[15] Ibid. *Foreign Assistance Act of 1973*, Section 32, 87 Statutes (1973): 733.

[16] Ibid.

[17] Henry Kissinger to Chilean Foreign Minister Carvajal, quoted in Peter Kornbluh, *The Pinochet File: A Declassified Dossier on Atrocity and Accountability,* (New York, 2003): 228. See also, Barbara Keys, "Congress, Kissinger, and the Origins of Human Rights Diplomacy," *The Journal of the Society for Historians of American Foreign Relations Online,* http://www.academia.edu/5433047/Congress_Kissinger_and_the_Origins_of_Human_Rights_Diplomacy (accessed March 11, 2015).

[18] Subcommittee on International Organizations and Movements of the House Committee on Foreign Affairs, "Human Rights in the World Community: A Call for U.S. Leadership," 93d Congress, 2nd Sess., (1974): 9-10, http://catalog.hathitrust.org/Record/003213998 (accessed December 11, 2014).

[19] Cohen, "Human Rights Practices" *The American Journal of Int'l Law*, 253.

[20] Ibid.

[21] Cristy Passman, *International Security Assistance and Arms Export Control Act of 1976*, Online 2 Md. J. Int'l L. 169 (1977): 170-172, http://digitalcommons.law.umaryland.edu/mjil/vol2/iss2/5 (accessed December 11, 2015).

[22] Ibid.

[23] Cohen, "Human Rights Practices" *The American Journal of Int'l Law*, 260.

[24] Ibid.

[25] Ibid.

[26] Ibid.

role in advancing human rights around the world.[27] But the DoS professional bureaucracy stymied the President's endeavors.[28] This arguably occurred because the career Foreign Service had an "organizational essence," that perceived its primary mission as the "maintenance of smooth and cordial relations with other governments;"[29] DoS did not accurately report information about foreign governments;[30] and, DoS exaggerated the importance of U.S. interests in countries where there were allegations of gross human rights abuses.[31]

President Reagan and the first President Bush took a foreign relations approach that was reminiscent of Presidents Nixon and Ford. Evidenced in many ways, an excellent example of the foreign assistance and training policies and practices of their administrations is found in the training conducted at the United States Army School of the Americas.[32] According to the United States Government Accounting Office (GAO), over 61,000 security force personnel were trained by the School of the Americas.[33] During President Reagan and President Bush's tenure in the 1980s, approximately one third of the students were from El Salvador, and in the 1990s, more than 50 percent came from El Salvador, Chile, Colombia, Panama, Peru, and Nicaragua.[34] The security forces of the aforementioned Latin American countries during these years accumulated some of the worst documented gross violations of human rights.[35] In fact, after vehemently denying for years that torture, execution and other potential gross violations of human rights were being taught at the School of the Americas, in September 1996, the United States military released copies of seven training manuals that had been used for a decade and contained instruction in Spanish on how to blackmail, torture and execute.[36]

The Leahy Laws

After more than twenty years of extensive and pervasive efforts to include human rights considerations in a wide variety of authorizations and appropriations, Congress, under the leadership of Senator Patrick Leahy from Vermont, mandated foreign assistance and military training be predicated on a clean record, i.e., one absent of human rights violations. Senator Leahy inserted what is commonly called the Leahy Amendment into the 1997 DoD *Appropriations Act* after it was revealed that foreign assistance and training had been given to the Colombian government. Evidence

---

[27] Office of the Historian United States Department of State, "Milestones: President Carter and Human Rights, 1977-1981," https://history.state.gov/milestones/1977-1980/human-rights (accessed February 2, 2015).

[28] Cohen, "Human Rights Practices," *The American Journal of Int'l Law*, 257.

[29] Ibid.

[30] For example, despite credible evidence that a hundred thousand, or more, people in East Timor had been killed by Indonesian military forces, the State Department asserted that these were inaccurate, over-inflated reports, and that in fact very few had died in East Timor. The department also argued that those who had died were actually Marxist terrorists, and that the abuses were not widespread or systematic, but merely the actions of isolated local commanders. Ibid., 259.

[31] In one instance, with respect to a proposal to triple military assistance to the Philippines, it was asserted that Philippine President Ferdinand Marcos would close U.S. bases, despite agreements that did not contractually end for more than another decade. Experts widely discounted such assertions. Ibid., 260.

[32] The School of the Americas was renamed The Western Hemisphere Institute for Security Cooperation in 2001 after calls to close the School of the Americas for training gross human rights violators, among other reasons. See Amnesty International, "Unmatched Power, Unmet Principles: The Human Rights Dimensions of U.S. Training of Foreign Military and Police Forces," *2002 Report of Amnesty International, Amnesty International USA* (Fall 2002): 10, 35-38, http://www.amnestyusa.org/pdfs/msp.pdf (accessed December 11, 2014).

[33] United States Government Accounting Office, "School of the Americas: U. S. Military Training for Latin America Countries," *United States Government Accounting Office Report to Congressional Requestors*, GAO/NSIAD 96-178, (August 22, 1996): 4-6, http://www.gao.gov/assets/230/223141.pdf (accessed December 11, 2014).

[34] Ibid., 6-8.

[35] Bill Quigley, "The Case for Closing the School of the Americas." Online *20 BYU J. Pub. L. 1* (2005-2006): 4-7, http://digitalcommons.law.byu.edu/cgi/viewcontent.cgi?article=1355&context=jpl (accessed December 11, 2014).

[36] Amnesty International, "Unmatched Power, Unmet Principles: The Human Rights Dimensions of U.S. Training of Foreign Military and Police Forces," 36-37.

disclosed that even though President Clinton's administration denied aid had been given to Colombian Army and security forces in 1994, the administration's assurances were false.[37]

Over the next twenty years the scope of the Leahy Laws expanded. The initial 1997 language applied to Counter Narcotics Control funding, and required vetting for human rights allegations. In 1998, the law included all security assistance funding from the *Foreign Assistance Act* of 1961[38] and DoD appropriations for military training were added to the human rights vetting requirements.[39] The Leahy Laws have evolved over the decades, with the most recent changes found in the 2011 DoS and 2014 DoD Leahy Laws.

The Leahy Laws are found in two places, the *Foreign Assistance Act* of 1961 and in the DoD *Appropriations Act*. They mandate human rights vetting for beneficiaries of aid from the *Foreign Assistance Act*, the *Foreign Export Control Act*, or recipients of military training, equipment, or other assistance from the DoD. The current version of the Leahy Law in the *Foreign Assistance Act*, Title 22, United States Code, 2378d, Section 620M (a), provides:

> (a) In General.-No assistance shall be furnished under this Act or the Arms Control Act to any unit of the security forces of a foreign country if the Secretary of State has credible information that such unit has committed a gross violation of human rights.[40]

Although similar, the DoD *Appropriations Act* Leahy Law states, in pertinent part:

> (a) In General –
> (1) None of the funds made available by this Act may be used for any training, equipment, or other assistance for the members of a foreign security force if the Secretary of Defense has credible information that the unit has committed a gross violation of human rights.
> (2) The Secretary of Defense, in consultation with the Secretary of State, shall ensure that prior to a decision to provide training, equipment, or other assistance to a unit of a foreign security force full consideration is given to any credible information available to the Department of State relating to human rights violations by such unit.[41]

Significantly, although there are exceptions to these requirements in each of the two laws, the exception in each law is slightly different. In the *Foreign Assistance Act*, if there is credible information of a gross human rights violation, assistance may still be provided if the Secretary of State determines "the government of such country is taking effective steps to bring the responsible members of the security forces to justice."[42] The DoS does not consider transferring individual members of a military unit or security force out of that unit an "effective step" within the intent of the law. A formal investigation into the conduct of the accused unit or individual is likewise not considered an effective step in bringing the individual to justice.[43] In the Defense *Appropriations Act*, the training, equipping, and assisting prohibition may not apply if the Secretary of Defense, "in consultation with the Secretary of State, determines that the government of such country has taken

---

[37] Carlos Salinas, "Colombia in Crisis," *Foreign Policy in Focus Online*, 5, no. 5, (March 2000): http://www.ciaonet.org/pbei/fpif/sac01/index.html (accessed March 9, 2015).

[38] Amnesty International, "Unmatched Power, Unmet Principles," 36-37.

[39] Ibid.

[40] Title 22, United States Code 2378d, Section 620M, Subdivision (a), *Foreign Assistance Act of 1961*, https://www.law.cornell.edu/uscode/text/22/2378d (accessed January 22, 2015).

[41] Public Law 113-76, Division C, Consolidated Appropriations Act, Section 8057, Subdivision (a)(1) and (a)(2), Defense Department Appropriations Act (2014), http://www.gpo.gov/fdsys/pkg/BILLS-113hr3547enr/pdf/BILLS-113hr3547enr.pdf (accessed January 22, 2015).

[42] Title 22, United States Code 2378d, Section 620M, Subdivision (b), of the Foreign Assistance Act of 1961, https://www.law.cornell.edu/uscode/text/22/2378d (accessed January 22, 2015).

[43] United States Government Accounting Office, "Human Rights: Additional Guidance, Monitoring, and Training Could Improve Implementation of the Leahy Laws." United States Government Accounting Office, Report to Congressional Requestors, GAO-13-866 (September 25, 2013), http://www.gao.gov/products/GAO-13-866 (accessed February 26, 2015).

all necessary and corrective steps or other assistance is necessary to assist in disaster relief operations or other humanitarian or national security emergencies."[44]

Unlike DoS, DoD provides guidance that removing an individual accused of gross violations of human rights from a unit could be a corrective and necessary step. Also, DoD opines that human rights training for the unit or the accused, as well as a combination of training and removal from the unit in the case of an individual or individuals, could constitute "all necessary and corrective steps within the meaning of the law."[45]

Despite these definitional and interpretative differences, both DoS and DoD reported to the GAO that as of September 2013, DoS had never used the statutory exception contained in the *Foreign Assistance Act* Leahy Law. Moreover, DoD had never conducted training pursuant to a foreign government taking all necessary corrective steps to remediate allegations of security force violations of human rights.[46] However, the training could take place given the remediation definition of DoD. Training in human rights, as outlined above and in the recommendations below, could constitute the "necessary steps" and allow additional, traditional U.S. military training of such foreign units and individuals.

In 2011, the *Foreign Assistance Act* Leahy Law was amended to add seven procedural requirements to accommodate the DoS. First, they must retain a list of all units being trained by country. The second requirement is that the department facilitate processing "credible information" from non- U.S. government sources. Third, they must routinely request and obtain information about credible allegations of gross violations of human rights from DoD, the Central Intelligence Agency, and other U.S. government sources. Fourth, the department must ensure the information received from all sources is evaluated and preserved. Fifth, they are required to ensure that if an individual is vetted, the appropriate security force unit is also vetted. The sixth requirement is that attempts must be made to identify the unit involved when credible information of a gross violation exists, but the responsible unit is unknown. Finally, to the extent possible, the DoS must provide to the public the identity of individuals and units to which assistance or training are denied as a result of the law.[47] Also in 2011, Congress changed the standard for the quantum of evidence of a gross violation from "credible evidence" to "credible information" stating that they did not intend that the evidence must be admissible in court and the statute was changed so that "a [single] violation" rather than "[multiple] violations" would trigger the prohibition.[48]

No similar provisions were added to the DoD Leahy Law, but in 2014, that law was amended to add equipping and assistance to the training prohibition, providing, in pertinent part, "any training, equipment, or other assistance for the members of a unit of a foreign security force if the Secretary of Defense has credible information that the unit has committed a gross violation of human rights."[49]

---

[44] Public Law 113-76, Division C, Consolidated Appropriations Act, Section 8057, Subdivision (b), Defense Department Appropriations Act (2014), http://www.gpo.gov/fdsys/pkg/BILLS-113hr3547enr/pdf/BILLS-113hr3547enr.pdf (accessed February 26, 2015).

[45] DOD Joint Staff policy message, Human Rights Verification for DOD-Funded Training of Foreign Personnel, DTG 071300Z Jun 04, http://www.disam.dsca.mil/documents/itm/functional_areas/human_rights/dod_memo_human_rights_verification.pdf (accessed February 22, 2015).

[46] United States Government Accounting Office, "Human Rights," GAO-13-866, 6-7.

[47] Ibid., 5-6.

[48] Nina M. Serrafino, June S. Beitel, Lauren Ploch Blanchard, and Liana Rosen, "'Leahy Law' Human Rights Provisions and Security Assistance: Issue Overview." *Congressional Research Service Online*, (January 29, 2014): 4, http://www.fas.org/sgp/crs/row/R43361.pdf (accessed December 11, 2015).

[49] Ibid.

The GAO, at the request of Senator Leahy and other members of Congress conducted a yearlong audit in fiscal year 2013 to review the implementation of the Leahy Laws by DoS and DoD. The GAO found that, among other things, while guidance had been provided for some of the original requirements of the Leahy Law, all of DoS training materials were out of date regarding information about the 2011 amendments, most notably the new procedural requirements for obtaining, processing and storing vetting information.[50]

With respect to training, perhaps even more perplexing were the findings that the DoS Leahy Law vetting training was contained in two web based, on-line courses, both of which were optional for vetting personnel, and which had to be personally paid for by DoS personnel who did not have an additional duty assignment as a Leahy Law human rights Vetter. In fact, there had been requests that the training courses be available to DoS personnel free of charge, but the requests were denied by the Foreign Service Institute.[51]

The Leahy Laws Vetting Process

DoS is responsible for conducting vetting of military and security force units and individuals for both the *Foreign Assistance Act* and the Defense *Appropriations Act* human rights programs.[52] Since it began in 1997, the DoS vetting process has evolved into a web based computer system entitled the International Vetting and Security Tracking System (INVEST).[53] Since the inception of the INVEST program in 2010-2011, about 400,000 units and individuals have been screened for training with the U.S. military, averaging 130,000 reviews a year. Significantly, the rate of vetting is increasing, with approximately 162,000 vetted through 159 embassies in fiscal year 2012.[54]

DoS, in conjunction with DoD and other government agencies, processes requests for vetting from the military or other sponsoring agency. This is done primarily through the embassies, where the credibility of information about gross violations of human rights is assessed. The information and embassy analysis is processed through DoS Bureau for Democracy, Human Rights, and Labor (DRL) in Washington, DC, the responsible bureau for vetting. Two separate processes exist: one for training and one for equipment and assistance. [55]

Embassy vetting procedures vary from embassy to embassy; there is no Department wide Standard Operating Procedure (SOP), although each embassy is encouraged to have its own SOP.[56] DoS "does not monitor whether all U.S. embassies have required SOPs that address State and DoD Leahy law requirements," and DRL in Washington, DC had only reviewed 43 of the SOPs out of 159 embassies that conducted Leahy vetting.[57] During the 2013 audit, the GAO visited eight embassies in diverse geographic locations and found that two of the embassies wrote their SOPs while the audit was taking place and the other six significantly modified theirs during the audit.[58]

Definitions of key terms such as *training*, *security forces*, *credible information*, and *gross violation of human rights* are arguably impacted by subjective interpretation for purposes of the vetting process. With respect to *credible information*, for example, the GAO stated, "State guidance provides latitude in evaluating the credibility of information and advises personnel conducting

---

[50] United States Government Accounting Office, "Human Rights," GAO-13-866, 21-22.
[51] Ibid.
[52] Nina M. Serafino, et al., "'Leahy Law' Human Rights Provisions and Security Assistance: Issue Overview," 7.
[53] United States Government Accounting Office, "Human Rights," GAO-13-866, 8-9.
[54] The Secretary of State, *Congressional Budget Justification for Fiscal Year 2014, Volume 1: Department of State Operations* (2013): 261, http://www.state.gov/documents/organization/207266.pdf (accessed February 18, 2015).
[55] United States Government Accounting Office, "Human Rights," GAO-13-866, 8-10.
[56] Ibid., 19-21.
[57] Ibid.
[58] Ibid.

human rights vetting to exercise good judgment and common sense."[59] Likewise, with respect to the definition of a *gross violation of human rights*, the auditors observed that DoS "notes that the Leahy Laws do not contain a definition of 'gross violation of human rights.'" Consequently, they noted, "State, therefore, uses the definition included in Section 502B(d) of the *Foreign Assistance Act* of 1961 as its working standard."[60] This is ironic, since *Foreign Assistance Act* section 502B was said to be too difficult to implement in light of the ambiguity of the definition of human rights violations, and that assertion by the Executive led to other human rights legislation, including the Leahy Laws.

Perhaps the most significant definitional issue arises from *training*. While a definition would appear to be straight forward, there is considerable flexibility with respect to the term.[61] The Defense Institute of Security Management (DISAM) states that "training" includes, among other things: "Joint Combined Exercise Training (JCET); Counternarcotics Training; Counter-narco-terrorist Training; Humanitarian Demining Training; DOD Combating Terrorism Fellowship Program (CTFP); Any training activities conducted under the Combatant Commander's Initiative Fund; U.S.-Sponsored training programs, to include the International Military Education and Training Program (IMET) and FMS-purchased training at DOD educational institutions."[62]

On the other hand, "training" does not include, among other things: "Exercises, Individual or Subject Matter Expert Exchanges; Mil-To-Mil Contacts; Seminars and Conferences; Partnership and other small unit exchanges where the primary focus is interoperability or mutually beneficial exchanges and not training of foreign security forces; bona fide familiarization and orientation visits; or, Pre-deployment site surveys (PDSS) or other planning and coordination visits supporting the Joint Combined Exchange Training (JCET) or training event."[63] Interestingly, the United States Army JAG Corps publishes an Operational Law Handbook that attempts to address the distinction. Compare the following examples of training and non-training, respectively, within the meaning of Security Assistance:

> Interoperability and Safety: A month-long Combined Airborne Parachute Exercise with other countries, whose participating troops are all airborne qualified in their own countries, a 2-hour block of instruction on C-130 entry and egress safety procedures would be Interoperability Training ("Little t" training), since the primary purpose is safety and interoperability of the foreign troops. Additionally, it is a short duration (2 hours) training event, the cost is not significant, and their level of training is not significantly enhanced (since the foreign troops are already airborne qualified). Therefore, this would likely be classified as Interoperability, Safety, and Familiarization Training, and DOD may fund this training with its own O&M funds.
>
> Security Assistance Training: On the other hand, training foreign troops on airborne operations, including the provision of DOD trainers for a month-long airborne school to qualify all the individual foreign troops in airborne jumps, would likely be classified as Security Assistance Training ("Big T" training). In this case, the duration of the training is long (one month), the cost is likely significant, and most importantly, the level of training of the foreign troops is significantly increased. As a result, the primary purpose of the training is not the Interoperability,

---

[59] Ibid., 13.
[60] Ibid.
[61] Aaron Prince, "What is International Military Training?" *The DISAM Journal of International Security Cooperation Management Online*, Annual Volume 2 (August 2013), http://www.disamjournal.org/articles/what-is-international-military-training-850 (accessed February 26, 2015).
[62] Ibid.
[63] Ibid.

> Familiarization, and Safety of the foreign troops, and this training should be classified as Security Assistance training.[64]

As DISAM indicates in the published guidance for the military, "Even with current guidance, regulations, policies, and handbooks regarding the definition of international military training, it can still be difficult to determine 'Big T' training from 'Little t' training in certain circumstances." While wisely suggesting that military planners seek the advice and counsel of JAG officers and other experts with regard to definitional issues, the DISAM author cogently asks, "When does a seminar or conference cross over to training? Military Exercises might also include an element of training that would increase the foreign country's military capabilities; does this then cross over into the 'Big T' training definition?"[65]

Another significant issue is funding for Leahy vetting. DoS budgets for an average of 130,000 vetting actions per year, but the rate of vetting is increasing, with approximately 162,000 in fiscal year 2012. The rate of increased requests for vetting is expected to increase since the strategic goal is to have more international security partnership training, equipping and assistance. The budget for Leahy vetting was $2.75 million in FY 2014.[66] A twenty-five percent increase in vetting would require almost another million dollars during a time of fiscal austerity and shrinking budgets.

Recommendations

Although sound in principle, the Leahy Laws have unintended consequences that impede other important national security interests. Coalition partners who need the most training in human rights, rule of law, rules of engagement, and law of armed conflict may be prohibited from receiving that training from U.S. advisors; opportunities arise for other nations to fill the vacuum of U.S. military partnership; and, human rights receive less emphasis and are more likely to be violated by the military units that most need U.S. military training assistance. Thus, in order to achieve United States strategic policy goals for building regional partnerships, security coalitions, rule of law, and international human rights, the United States military must conduct more legal, special operations, and command training with foreign military forces than is permitted by the present interpretation of the Leahy Laws.

Strategic policy goals are most effectively accomplished by working with foreign military units, not by banning training to these units. A commitment to International Human Rights enhances U.S. international relations with allies, promotes international law, creates international credibility, and facilitates coalition building. The following recommendations would assist in reconciling the apparent conflict in training coalition units and individuals accused of gross violations of human rights:

- U.S. international military training should initially train coalition security forces in the Law of Armed Conflict, the Code of Conduct, effective Command and Control through Military Justice, and the consequences pursuant to international law for crimes that violate human rights; genocide, crimes against humanity and war crimes.

---

[64] *Operational Law Handbook, Chapter 14, Section IX, Fiscal Law*, International and Operational Law Department, The Judge Advocate General's Legal Center & School, U.S. Army Charlottesville, Virginia, (2012): 215-216, http://www.loc.gov/rr/frd/Military_Law/pdf/operational-law-handbook_2012.pdf (accessed March 11, 2015).

[65] Aaron Prince, "What is International Military Training?"*The DISAM Journal of International Security Cooperation Management.*

[66] Nina M. Serafino, et al., "'Leahy Law' Human Rights Provisions and Security Assistance: Issue Overview," 13.

- Include an express exception to the Leahy Laws vetting requirements for the aforementioned training by legal, special operations, and command trainers for units accused of gross human rights violations.
- Define training, credible information, and other essential terms clearly and unambiguously so they do not fall under the prohibitions imposed by the Leahy Laws.
- Define remediation and “effective steps” to “rehabilitate or bring to justice” to include the aforementioned training.
- Further research and analysis should be conducted to determine the impact and effectiveness of the Leahy Laws.

Permitting U.S. Special Operations Forces, Legal Officers and Commanders with Rule of Law, Human Rights Enforcement, and military justice experience to train partner nations in these essential military disciplines actually fulfills, rather than undermines the intent of the Leahy Laws. To accomplish that intent, the Laws must be amended and U.S. forces authorized to train foreign nation military units accused of human rights violations.

Army War College Review
Vol. 1, No. 3, Aug. 2015, 13-25

U.S. Army War College
Student Publications

The Islamic State: Terrorists or Millenarian Mass Movement?

Edward R. Sullivan

The Islamic State (IS) should be understood as an Islamist millenarian mass movement possessing broad anti-western appeal and an ideology distinct from Al-Qaeda. For more than a decade IS has deliberately and methodically worked to advance its cause. It grounds its message in solid theological roots, utilizing the Salafist ideology of Sayyid Qutb. Its ideology is one of revolution in which Islam is on par with communism and capitalism as a basis for societal organization. The clarity of its utopian social message of equality and brotherhood contrasts sharply with the chaos and cultural confusion attributed to globalization, making IS attractive to those susceptible to radicalization. Highly capable in media initiatives, IS nonetheless remains vulnerable to rogue messages that run counter to the desired image. Countering the ideology of the Islamic State is far more problematic than countering its organization. Increased international effort is needed. A failure to act now leaves the Arab and Islamic heartland in the hands of a methodical and capable cult-like organization whose continued existence directly undermines an already precarious regional stability.

Keywords: *ISIS, ISIL, Syria, Iraq, Islamists, Terrorism*

> A rising mass movement attracts and holds a following not by its doctrine and promises, but by the refuge it offers from the anxieties, barrenness and meaninglessness of an individual existence.
>
> —Eric Hoffer[1]

The emergence, growth, and victories of the Islamic State in Iraq and Syria (IS)[2] serve as dominant features of news programs and government briefings. Popular characterizations paint the group as

---

Edward R. Sullivan (M.S.S. United States Army War College) is a Lieutenant Colonel in the United States Marine Corps. *An earlier version of this article, written under the direction of Dr. Larry P. Goodson, earned a prestigious Marine Corps Association and Foundation General Thomas Holcomb Writing Award for the USAWC class of 2015.*

[1] Eric Hoffer, *The True Believer, Thoughts on the Nature of Mass Movements* (New York: Harper and Collins, 1951), 41.

[2] From the beginning, the group has been known variously as "Tawhid wa al-Jihad," "Al-Qaeda lil-Jihad fi Bilad al-Rafidain (QJBR), al-Qaeda in Iraq (AQI), the Mujahidin Shura Council, the Islamic State in Iraq (ISI), the Islamic State in Iraq and the Levant (ISIL), the Islamic State in Iraq and al-Sham (ISIS), and the anglicized version of the Arabic acronym "D'aesh" representing "The Islamic State in the region of al-Sham (Levant)." As the group itself abandoned any reference to locations in its name as of late 2014, throughout this paper it is referred to interchangeably as either the Islamic State or IS.

terrorists who opportunistically seized terrain and who are now trying to craft a state. Moreover, though they have decisively eclipsed Al-Qaeda, most people erroneously view the two groups as ideologically identical.[3] They are not. The activities and successes of the Islamic State to date are better understood as representative of a millenarian mass movement seeking to deliberately and fundamentally reshape society through violent revolution. Millenarianism is "the belief in a coming ideal society, especially in one brought about through revolutionary action."[4] For IS, this involves the violent recreation of God's Kingdom on Earth in keeping with a particular reading of select sacred texts. In this manner, IS assumes characteristics common to "cultic" religious militant movements throughout the world, such as Aum Shinrikyo in Japan; "the Covenant, the Sword, and the Arm of the Lord" in the United States; or certain Messianic Jewish groups in Israel, all seeking to bring down governments and systems they deem unlawful in order to create a utopian society.

Of foremost importance is the particular revolutionary message presented by IS together with the nature of the message's appeal. Legitimacy of the mission and the message can be everything to a terrorist organization,[5] particularly one demanding societal reordering. This necessitates consideration as to how (1) IS establishes itself in an Islamic context, (2) the IS "brand" is differentiated from the broader jihadist context, and (3) IS propagates its message to target recruits. The essay concludes with an assessment of future prospects.

Islam as an Ideology for Social Revolution

In 1964, Sayyid Qutb, an Egyptian member of the Muslim Brotherhood, wrote that:

> The leadership of mankind by Western man is now on the decline, not because Western culture has become poor materially, or because its economic and military power has become weak...the Western system has come to an end because it is devoid of those life-giving values which enabled it to be the leader of mankind. [6]

Written in prison, *Milestones* not only played a large role in bringing about Qutb's own execution by the Egyptian government in 1966,[7] but it became a foundational document and source of inspiration for Salafi Islamists across the world who portray Islam as a *political* ideology directly competitive with capitalism and communism. Many different "types" of Salafis exist, from "Establishment Salafis" to "Global Jihadists," differentiated largely by their willingness to work within non-Islamic systems and their dedication to a militarized revitalization of the *Ummah* or the community of believers.[8] As they pose the most pressing danger to the international community, this essay is concerned primarily with Global Jihadists, described by Tareq Abdelhaleem in *Global Jihadism* and ably represented by IS and Al-Qaeda leadership.[9]

---

[3] Graeme Wood, "What ISIS Really Wants," *The Atlantic online*, March 2015, http://www.theatlantic.com/features/archive/2015/02/what-isis-really-wants/384980/ (Accessed 25 February, 2015), 3.

[4] *Millenarianism* as defined by the *Merriam-Webster online dictionary*, http://www.merriam-webster.com/dictionary/millenarianism (Accessed January 21, 2015).

[5] Terrell E. Arnold, *The Violence Formula, Why people Lend Sympathy and Support to Terrorism*, (Lexington, MA: Heath, 1988), 151.

[6] Sayyid Qutb, *Milestones*, (USA: *SIME Journal*, 2005), 1 (Introduction).

[7] Ibid., 2 (Forward).

[8] Tareq Abdelhaleem, "The Counterfeit Salafis: Deviation of the Counterfeit Salafis," in *Methodology of Ahlul Sunnah L/al Jama'a*, (Dar Alargam, 2004), as cited in Jarret M. Brachman, *Global Jihadism: Theory and Practice*, (New York: Routledge, 2009), 26.

[9] Brachman spends considerable time differentiating "Global Jihadists" from other Salafi schools of thought, making a precise definition problematic. In general, Jihadists were originally inspired by the Al-Qaeda "Brand identity" created by Osama Bin Laden and share a more or less common set of seven characteristics in their religion and worldview. In Brachman's view, however, the word "global' was inappropriate prior to 2003. See Jarret M. Brachman, *Global Jihadism: Theory and Practice*, 39-48.

Global Jihadists (simply "Jihadists" henceforth) believe the first generations of Islam were an ideal time of harmony and brotherhood. This spiritual perfection was soon destroyed by theological innovation and ignorance of Islam's true path.[10] In Qutb's view, the first half of the profession of faith, "*la ilaha illa allah*" (there is no deity but God), is falsely equated in modern times with the 1st Commandant given to Moses, stating a belief in monotheism.[11] Qutb argued that in the Arabic of the Prophet's time, this "rejection of false deities" actually means a literal belief that there is "no sovereignty except God's, no law except from God, and no authority of one man over another, as the authority in all respects belongs to God."[12]

Jihadists at their core reject all elements of man-made governance; they reject borders, states, governments, and leaders delineated by anything other than God's law. In another seminal jihadist work, Abu Muhammad al-Maqdisi argues the theological case in *Democracy is a Religion*, namely that in democracy men submit themselves to the rule of other men who have taken on the role of deities as legislators and creators of laws.[13] This belief drives Islamists committed to Jihad to declare anyone believing in democracy to be a polytheist, as they ascribe to men powers rightfully belonging only to God.

At its core, Islam offers a utopian vision of social justice and equality. Like many utopian visions, however, significant differences exist between the theoretical ideal and the pragmatic reality. Jihadists strive to eliminate theoretical and pragmatic differences, believing that true social justice and equality among men is simply not possible until mankind is united under a flag of Islam, with "no other name . . . added to it, and '*la ilaha illa allah*' written on it."[14]

Like other radical ideologies promising a completely new future *if only* man were living by a different set of rules, the revolutionary ideology of Jihadists appeals to a specific type of person. Such a person is often susceptible to radicalization of almost any sort, regardless of the particular type of movement (i.e., communism, fascism, socialism, etc.). In what is increasingly a post-Marxist world, however, someone today wishing to fight against globalization and the liberal democratic ideology of the "West," essentially has a choice between either absolute anarchy or religious militancy, contemporaneously embracing the form of jihad.[15]

IS appeals to and attracts fanatics. But as Roger Griffin notes, "fanatic" in this case more accurately describes someone with unshakeable beliefs, displaying a calculating and single-minded, "rational" vision, incapable of self-doubt.[16] He argues that in a desperate fight to avoid *anomie* men create *nomos*, a "cosmic order" establishing the bounds of normative behavior that "predates humanity itself,"[17] promoting the belief that particular rules greater than ourselves govern the way life works. Within this construct, a "*nomic crisis*" occurs when this belief system appears to be under attack by the forces of modernity. Exported through the mechanisms of globalization, democratic liberalism is today breaking down more cultural traditions, transitioning populations from environments of well-defined moral choices to ones with an overabundance of decisions and a near

---

[10] Indeed Salafis get their name from the Arabic for "forefathers" or "predecessors" and in regular usage the name refers to the time of the companions of the prophet; meaning those who were alive during the time of Mohammed and the first four successors.

[11] Qutb, *Milestones*, 21.

[12] Ibid., 14.

[13] Abu Muhammad 'Aasim al-Maqdisi, *Democracy, a Religion*, pdf, http://www.kalamullah.com (Accessed 5 December, 2014), 11-12.

[14] As we clearly see with the Islamic State today. They have abandoned earlier versions of their flag to emulate exactly the kind of banner Qutb describes. Qutb, *Milestones*, 17.

[15] Brachman, *Global Jihadism*, 11.

[16] Roger Griffin, *Terrorist Creed* (New York: Palgrave Macmillan , 2012), 19.

[17] Ibid., 35.

absence of moral absolutes.[18] Overwhelmed by the possibilities stemming from this lack of clarity and feeling defenseless against what is seen as an attack on their culture and historic fundamental values, many people welcome the order, clarity, and discipline afforded by militant religious groups.[19]

Such an attraction exists regardless of the religion a person claims because it offers a way to fight back against globalization, unwelcome change, and feelings that old systems of order have broken down. As Jessica Stern suggests, "Although we see them as evil, religious terrorists know themselves to be perfectly good. To be crystal clear about one's identity, to know that one's group is superior to all others, to make purity one's motto and purification of the world one's life work—this is a kind of bliss."[20]

Not all who join the Islamic State are likely to leave home and start their journey believing fully in the cause of Jihad. Many may come because IS shows itself to be the most capable platform of anti-Western resistance in the world. Money and personal status can be drivers, though lower level fighters are normally not paid very well.[21] Others pursue jihad as a "fad" because it is seen as "cool" among Muslim youth.[22] Jihad is becoming the "great adventure" and a defining element of an Arab generation beset by chaos, warfare, and revolution. Many young people see their world in turmoil and under attack and blame the "Western" world.

In such populations, the search for noble purpose and moral clarity above all else can become quite common. Popular characterizations of Islamic radicals often espouse the view that they are drawn from among poor, disenfranchised, undereducated youth who reside in slums, but that is frequently not the case. As Eric Hoffer observed, the middle class more commonly recognizes fault and threat in the world, and seeks a reordering of society.[23] Seeing a lack of purpose in what potential recruits interpret as a sea of ambiguous social choices and potential outcomes often drive a person to value fraternity and community above individual freedoms.[24]

Hoffer's analysis may account for the appearance that IS has the most impact in "middle income" parts of the Middle East versus either end of the economic extreme.[25] It helps to explain why the Islamic State has taken hold in Syria and Iraq, supported by fighters from Tunisia, Jordan, and Morocco instead of Sudan or Qatar, and why it is more common in middle economic states of Europe rather than in Scandinavia or the Mediterranean periphery.[26] Hoffer notes, "It is not actual suffering but the taste of better things which excites people to revolt . . . frustration is greater when we have much and want more, than when we have nothing and want some."[27]

In Syria, the civil war exploded over demands for greater democracy and inclusiveness within the existing system, not from a desire for complete governmental change. Mass violence did not occur in Iraq until Sunnis determined that the paths to social mobility had opened, but not for them. Hoffer

---

[18] Jessica Stern, *Terror in the Name of God, Why Religious Militants Kill*, (New York: Harper Collins, 2003), 69.
[19] Ibid.
[20] Ibid., XXVIII.
[21] Ibid., 5.
[22] Ibid.
[23] "For men to plunge headlong into an undertaking of vast change, they must be intensely discontented yet not destitute, and they must have the feeling that by possession of some potent doctrine, infallible leader or some new technique, they have access to a source of irresistible power." Hoffer, *The True Believer*, 11.
[24] Ibid., 33.
[25] Peter R. Neumann, "Foreign Fighter Total in Syria/Iraq now exceeds 20,000; Surpasses Afghanistan Conflict in the 1980s," The International Centre for the Study of Radicalisation and Political Violence online, http://icsr.info/2015/01/foreign-fighter-total-syriairaq-now-exceeds-20000-surpasses-afghanistan-conflict-1980s/ (Accessed January 26, 2015), 1-2.
[26] Within the article the per capita rate per one million in population for participation with the Islamic State is 15 for Qatar and 100 for Sudan, as opposed to 1,500-3,000 for Tunisia and 1,500 for both Jordan and Morocco. For Europeans, contrast Italy and Sweden with 80 and 150 respectively, Germany with 500-600 and 440 for Belgium. Ibid., 1-2.
[27] Hoffer, *The True Believer*, 29.

concludes that in the contest to gain the support of those individuals open to radicalization, the group arriving first with the most complete and "perfected collective framework" wins.[28] The challenge for such groups lies primarily with distinguishing themselves from competitors.

Establishing Legitimacy

Through the broad use of social media, online magazines, and internet forums, IS spends significant effort to establish its "rightful place" as the vanguard of this millenarian revolution.[29] "The spark has been lit here in Iraq, and its heat will continue to intensify—by Allah's permission—until it burns the crusader armies in Dabiq." [30] This quote appears early in every magazine published by the Islamic State, acting as the title of the publication itself. It refers both to *Dabiq*, a town in the countryside near the Syrian city of Aleppo, and to the story of the apocalypse in Islam, wherein Jesus (*'Isa Ibn Maryam*) returns to lead the Muslim Armies against the armies of Rome—representative of "the West"—in northwest Syria.[31]

While IS and al-Qaeda share many common origins and doctrinal sources, IS demonstrates itself to be less a pure terrorist organization and more of a revolutionary movement. While Al-Qaeda focuses on a global jihad, IS turns almost all of its attention to securing the Arab World first (the near enemy) before shifting to enemies abroad (the far enemy).[32] Both seek the recreation of an Islamic Caliphate,[33] but differ with respect to the method and timing of the state's establishment. One of the more influential works in Jihadist literature is the book *Millat Ibrahim* by Abu Muhammed al-Maqdisi, which purports to lay out the correct path to establishing Islamic governance.[34] In al-Qaeda's interpretation, the fight against corrupt regimes (*taghut*/*tawaghit*)[35] appears less focused, targeting governments around the world and believing that once they are defeated a state will be declared and a leader chosen from among the faithful.

IS attacks this assertion directly, maintaining there can be no revival of the faith with the people living under a corrupt regime, and therefore a state with a just leader must be declared so the people are free to live under God's laws as they fight their oppressors.[36] They draw much of their argument from the early Meccan period in Islam, when the Muslim community was just starting out and found itself an outnumbered and unfavored minority. Mohammed served as the charismatic leader and exemplar to this early community, encouraging its migration to Medina and the establishment of a unified community under Islamic laws. Absent his leadership, had they fought the stronger tribes before consolidating their beliefs and religious practice in their own enclave, the community's

---

[28] Ibid., 41.

[29] Harleen K. Gambhir, "Dabiq: The Strategic Messaging of the Islamic State," August 15, 2014, *Institute for the Study of War*, http://www.understandingwar.org/sites/default/files/Dabiq%20Backgrounder_Harleen%20Final.pdf (Accessed September 16, 2014).

[30] *Dabiq: Issue 1 – The Return of Khalifah*, online, Ramadan, 1435, http://media.clarionproject.org/files/09-2014/isis-isil-islamic-state-magazine-Issue-1-the-return-of-khilafah.pdf (Accessed September 16, 2014), 2.

[31] Ibid., 4.

[32] Fawaz Gerges as quoted by Scott Shane and Ben Hubbard, "ISIS Displaying a Deft Command of Varied Media," *New York Times online*, August 30, 2014, http://www.nyti.ms/1qQ8tQD , (Accessed February 8, 2015), 3.

[33] A Caliphate or *Khilafah*, is an Islamic Government led by a Caliph, a successor of the Prophet Muhammed as both the political and religious head of state. The battle between who may be the Caliph and what the qualifications for the position are forms a key element of the fundamental schism between Shia and Sunni Islam.

[34] The book itself can be found using the following information and link, Abu Muhammed 'Asim Al-Maqdisi, "Millat Ibrahim (The Religion of Ibrahim) and the Calling of the Prophets and Messengers, and the Methods of the Transgressing Rulers in Dissolving it and Turning the Callers away from it, (2nd ed.)," (at-Tibyan Publications, date not given, but early to mid-1990s), pdf file, online, http://www.kalamullah.com/al-maqdisi.html (accessed 5 December, 2014).

[35] Corrupt regimes in this case refers to any forms of government other than a properly formatted Islamic theocracy. Chief sins of the tawaghit include democracy, idolatry, nationalism, and polytheism by virtue of the embrace of democracy.

[36] Author not Given, "Part 3: The Concept of Imamah is from the Millah of Ibrahim," *Dabiq: Issue 1*, 24.

prominence might not have happened. Reinforcing such connections, soon after declaring the establishment of the Islamic State in ash-Sham (the Levant) in late June/early July 2014, their leader, Abu Bakr al-Baghdadi, took the name of the man to whom God originally gave responsibility for leading the faithful and became known as Caliph Ibrahim (Abraham of the Bible).[37]

As an organization, the Islamic State is not new. They follow a lineage beginning more than a decade ago under the leadership of Abu Mus'ab az-Zarqawi (AMZ) in western Afghanistan. Following the invasion of Iraq by U.S.-led forces in 2003, AMZ first shifted his operations from Afghanistan to Kurdish areas before moving to western Iraq and al-Anbar Province.[38] Though initially under different names, the group was widely known as Al-Qaeda in Iraq (AQI) until late 2006, when in October it declared itself the Islamic State of Iraq (ISI) under Abu 'Umar al-Baghdadi, following the death of AMZ months earlier.[39]

In the initial issue of *Dabiq* magazine, IS devotes seven full pages to describing how it arrived to the present day by faithfully adhering to a plan to reestablish the Caliphate as laid out prior to 2004 by AMZ. Put in English terms, AMZ laid out a five phase plan: 1) emigration of fighters to a safe haven; 2) creation of fighting groups; 3) destabilization of existing regimes through creation of chaos; 4) consolidation of areas under group control; 5) establishment of a Caliphate.[40] In recounting the plan within *Dabiq*, its importance is made clear in separate bold text that states: "This has always been the roadmap towards *Khilafah* for the mujahidin."[41] In this regard at least, they are not simply rewriting history to suit events as they happen. The U.S. military captured a February 2004 letter from AMZ to Al-Qaeda Senior Leadership (AQSL) laying out the plan in some detail and making clear that AMZ's group offered to *cooperate* with AQSL, acting as a "vanguard" or "bridge" toward realizing the caliphate.[42] Within the letter, AMZ states that if AQSL agrees with his plan, "we will be your readied soldiers, working under your banner, complying with your orders, and indeed swearing fealty to you publicly and in the news media. . ."[43]

Such communications are at the heart of the IS argument that they are the true leaders of the Global Jihad and that Al-Qaeda has lost its way. By early February 2014, AQSL took the unprecedented step of publicly repudiating ISIS, stating the two groups shared no connections after public allegations that ISIS was broadly refusing to heed direction from AQSL.[44] By December 2014, IS devoted the majority of Issue 6 of *Dabiq* to ideological attacks on Al-Qaeda.[45] Contradictions in statements by Al-Qaeda leader Ayman al-Zawahiri and key regional subordinates form the basis of an extensive article in which AQSL leadership was cast as theologically ignorant, lacking both clarity of thought and devotion to the cause displayed by IS leaders. A second and equally substantial article offered the personal testimony of a former al-Qaeda fighter regarding the group's ineptitude and

---

[37] Harleen Gambhir, "Dabiq: The Strategic Messaging of the Islamic State," 5.

[38] Author not Given, "From Hijrah to Khilafah," *Dabiq: Issue 1*, 36.

[39] Brian Fishman, "Fourth Generation Governance – Sheikh Tamimi defends the Islamic State of Iraq," March 23, 2007. *Combating Terrorism Center at West Point*, Journal article, https://www.ctc.usma.edu/posts/fourth-generation-governance-sheikh-tamimi-defends-the-islamic-state-of-iraq (Accessed September 16, 2014).

[40] Author not Given, "From Hijrah to Khilafah," *Dabiq: Issue 1*, 36-40.

[41] Ibid., 38.

[42] Abu Mus'ab az-Zarqawi, "February 2004 Coalition Provisional Authority English translation of terrorist Musab al-Zarqawi letter obtained by United States Government in Iraq," online, http://2001-2009.state.gov/p/nea/rls/31694.htm (accessed 10 January 2015).

[43] Ibid.

[44] Liz Sly, "Al-Qaeda disavows any ties with radical Islamist ISIS group in Syria, Iraq," *Washington Post online*, February 3, 2014, http://www.washingtonpost.com/world/middle_east/al-qaeda-disavows-any-ties-with-radical-islamist-isis-group-in-syria-iraq/2014/02/03/2c9afc3a-8cef-11e3-98ab-fe5228217bd1_story.html, (Accessed February 22, 2015).

[45] *Dabiq: Issue 6 – Al-Qaeda of Waziristan*, online, Rabi' al-Awwal, 1436, http://media.clarionproject.org/files/islamic-state/isis-isil-islamic-state-magazine-issue-6-al-qaeda-of-waziristan.pdf (Accessed 10 January 2015).

failures in Waziristan.[46] Throughout the publication, IS paints Al-Qaeda as (a) overly willing to accept compromise and leniency for the sake of military expediency in the cause of jihad, and (b) as a group lacking any plan beyond fighting a global terrorist campaign.[47]

When seeking to ground their arguments in theology, next in importance to Muslims after the Koran are the *Hadith*, a collection of verified eyewitness accounts of what the Prophet Mohammed said and did regarding various topics.[48] Hadith, however, are not all treated equally. Particular hadith are chosen from two authors known as the *Sahihain* typically accorded the greater weight. In the first installment of *Dabiq*, IS uses direct Koranic verses and hadith from the *Sahihain* almost exclusively, attempting to make its case for establishment of the State more difficult to assail on theological grounds alone.[49] IS consistently establishes its ideological position using only solid theological arguments within communications such as *Dabiq*. As Graeme Wood argues, "...the Islamic State is Islamic. *Very* Islamic . . . the religion preached by its most ardent followers derives from coherent and learned interpretations of Islam."[50]

As a result of these and other factors, the group now rules a de facto state carved from Iraq and Syria. IS controls significant territory, provides a range of government services,[51] mints its own currency,[52] and operates a military apparatus that aspires to have a monopoly on the use of violence within its borders—which is far more state-like than anything Al-Qaeda has achieved. Though no foreign governments have recognized IS, the group regularly trumpets pledges of loyalty from jihadist groups around the world. In fact, *Dabiq: Issue 5* titled simply "Remaining and Expanding" contains statements and photos of loyalists in "new *wilayat* (provinces)" in Egypt (Sinai), Saudi Arabia, Yemen, Algeria, Libya, Indonesia, Nigeria, and the Philippines, among others.[53] The Islamic State is enjoying undeniable success in establishing its legitimacy among jihadist elements, placing it at the forefront of a jihadi mass movement forcing social revolution. On the most basic level "success breeds success" and since the fall of the Iraqi city of Mosul in the summer of 2014 nearly all jihadists traveling to Iraq are joining IS.[54]

Spreading the Message

The arrival of a "new era" is proclaimed in the inaugural issue of *Dabiq* magazine with words attributed to Shaykh Abu Muhammad al-Adnani:

> The time has come for those generations that were drowning in oceans of disgrace, being nursed on the milk of humiliation, and being ruled by the vilest of people, after their long slumber in the darkness of neglect—the time has come for them to rise.[55]

---

[46] Abu Maysarah as-Shami, "The Qa'idah of Adh-Dhawahiri (Zawahiri), Al-Harari, and An-Nadhari,and the Absent Yemeni Wisdom," 16-25. And Adu Jarar ash-Shamali, "Al-Qaeda in Waziristan: a Testimony from Within," and 40-55, *Dabiq: Issue 6 – Al-Qaeda of Waziristan*.

[47] Abu Maysarah as-Shami, "The Qa'idah of Adh-Dhawahiri (Zawahiri), Al-Harari, and An-Nadhari,and the Absent Yemeni Wisdom," *Dabiq: Issue 6 – Al-Qaeda of Waziristan*, 16-25.

[48] Harleen Gambhir, "Dabiq: The Strategic Messaging of the Islamic State," 6.

[49] Ibid., 6.

[50] Graeme Wood, "What ISIS Really Wants," 5.

[51] Aaron Zelin, "The Islamic State of Iraq and Syria Has a Consumer Protection Office," *The Atlantic online*, June, 2014 http://www.theatlantic.com/international/archive/2014/06/the-islamic-state-of-iraq-and-syria-has-a-consumer-protection-office-372769/, (Accessed October 8, 2014), 1-3.

[52] Author not given, "The Currency of the Khilafah," *Dabiq: Issue 5 – Remaining and Expanding*, online, Muharram, 1436 http://media.clarionproject.org/files/islamic-state/isis-isil-islamic-state-magazine-issue-5-remaining-and-expanding.pdf (Accessed January 10, 2015), 18.

[53] Author not given, "Remaining and Expanding," *Dabiq: Issue 5 – Remaining and Expanding*, 22-33.

[54] Scott Shane and Ben Hubbard, "ISIS Displaying a Deft Command of Varied Media," 2.

[55] Abu-Muhammed al-Adnani al-Shami, *Dabiq: Issue 1*, 9.

While such imagery is used by both Al-Qaeda and the Islamic State in media products, striking contrasts exist between both the production quality and content associated with the two groups. IS production values are top-notch, and the speed with which they incorporate recent events into their products is impressive. Al-Qaeda's *Inspire* magazine remains closer to a how-to manual for aspiring jihadists, whereas *Dabiq* seeks to educate, justify, influence, and inform.[56] Both groups study marketing, actively injecting "game theory" into web forums complete with levels, points, and associated privileges to encourage more active participation.[57] IS goes a step further, producing jihadist video games that capture the allure and themes of popular online games such as "Call of Duty" and "Grand Theft Auto."[58] In terms of their media operations, one RAND analyst stated succinctly, "Al-Qaeda is like AOL. The Islamic State is Google."[59]

The element of theater plays a large role in propagating messages of terror. Video beheadings of captives, disturbingly commonplace by the end of 2014, are an excellent example. The clean production values, the choice of an executioner with a British accent, apparently well-kept prisoners being killed through beheading with a small knife versus a sword—all are calculated efforts to terrorize the West and embolden potential recruits.[60] Sending a message, rather than just committing an act tailored to strike at the core of Western fears, is the goal.[61]

Of all of the messaging platforms, people in the West are most familiar with the videos—or more accurately excerpts from those videos. Most people in the developed world do not normally stumble onto jihadist web forums or peruse IS publications, but if the group can make an action horrific enough, and with high production values, the nightly news broadcast it on their behalf. Poor quality audio or video might get only a verbal description, whereas high quality productions are more likely to be shown to the target audience with only a small pixilated section masking the carnage.

The February 2015 release of a much longer than normal video showing captured Jordanian pilot First Lieutenant Muath Al-Kaseasbeh being burned alive inside of a cage demonstrates the relationship between media quality and international coverage. For days preceding the release of the video, news networks around the world tried to discern the extent of negotiations between IS and the Jordanian government, and the story ran regularly on multiple channels. When it looked as though a deal might have been possible, IS released a 22-minute cinematic quality production targeting Arabs rather than the West, which guaranteed through its savagery that it would dominate the news for days if not weeks. Perhaps beheadings had become too commonplace, or perhaps IS sought to put extra stress on the Jordanian regime, which already was facing a hostile public due to the war, but within ten minutes of the public release, IS distributed talking points justifying their use of fire on a captive.[62] For days every news program showed the moments before and after the pilot was

---

[56] "Dabiq: The Strategic Messaging of the Islamic State," 1-2.mk

[57] Jarret Brachman and Alix Levine, "The World of Holy Warcraft, How Al-Qaeda is using online game theory to recruit the masses," *Foreign Policy online*, April 13, 2011, http://www.foreignpolicy.com/articles/2011/04/13/the_world_of_holy_warcraft , (Accessed December 4, 2014).

[58] Terrence McCoy, "The Islamic State's 'Call of Duty' Allure," *The Washington Post online*, October 28, 2014, http://washingtonpost.com/news/morning-mix/wp/2014/10/28/the-islamic-states-call-of-duty-allure , (Accessed December 5, 2014).

[59] Colin Clarke, as quoted in Josh Kovensky, "ISIS's New Mag Looks Like a New York Glossy-with Pictures of Mutilated Bodies," *New Republic Online*, August 25, 2014, http://www.newrepublic.com/article/119203/isiss-dabiq-vs-al-qaedas-inspire-comparing-two-extremist-magazines , (Accessed October 8, 2014).

[60] Robert D. Kaplan, "Terrorism as Theater," *Stratfor Global Intelligence online*, August, 27, 2014, http://www.stratfor.com/weekly/terrorism-theater/ ,(Accessed September 16, 2014), 1.

[61] Ibid., 1.

[62] Duncan Gardham and John Hall, "Was Jordanian Pilot Burned Alive after sick twitter campaign among ISIS supporters to name his method of death?" *Daily Mail Online*, February 4, 2015, http://www.dailymail.co.uk/news/article-2939196/was-jordanian-pilot-burned-alive-sick-twitter-campaign-ISIS-supporters-method-death.html , (Accessed February 8, 2015).

killed, and some posted the entire video unedited for those wishing to view it on their computers—exactly the media impact and reaction sought by the Islamic State.

By again referencing scriptural examples, IS justified its actions against the pilot citing immolation as a legitimate method, concluding that if done in *mumathala* (reciprocity) it was acceptable.[63] The choice of the execution site at a building previously bombed by the coalition, the trapping of the captive inside of a cage, his death by fire, and the subsequent piling of building rubble upon his corpse were all specifically chosen to depict "just" retribution for "innocent civilians" caught inside buildings, burned and buried by coalition airstrikes.[64] Immediately after the capture of the pilot IS launched a twitter campaign under the title #SuggestAWayToKillTheJordanianPilotPig that received thousands of responses, and among them was burning him alive and burying him under rubble.[65] The solicitation of fresh methods of execution, the tailored extended video production, and the sheer brutality of the killing gave IS exactly the publicity they desired. Presumably, in their calculations, what they lose in popularity through this act will be trumped by what they gain through continued violence and fear.[66] Shock value keeps their video messages at the forefront, and that means a continual escalation of barbarity in future killings to retain world attention.[67]

The IS magazine *Dabiq*, a monthly publication first distributed online early in July 2014, is more traditional. All issues are very high quality, with complex text and photo layouts and top-notch graphics. Most, though not all, of the language is either written or proofed by native English speakers to ensure clarity and deflect criticism.[68] The titles of the issues act as the guiding themes and show logical messaging progression:

- Issue 1: "The Return of Khilafah," supports the creation of the Islamic State today and advances an overall plan of action moving forward.
- Issue 2: "The Flood," focuses on the choice to support and participate in the Islamic State, or risk being swept away in a new cleansing of the Earth.
- Issue 3: "A Call to Hijrah," explains why Muslims must migrate from foreign lands and make their homes in the State in order to normalize life and state administration.
- Issue 4: "The Failed Crusade," shows the IS flag in St. Peter's Square in the Vatican. The most overtly military issue to date, it focuses on "failed" U.S. strategy in the region as well as signs of Armageddon.
- Issue 5: "Remaining and Expanding," details the establishment of new Provinces throughout the Islamic world, supported with photos and individual statements of loyalty.
- Issue 6: "Al-Qaeda of Waziristan" is dedicated to a lengthy and detailed denunciation of Al-Qaeda as a jihadist organization.

Among other features, each issue contains a section of at least two pages entitled "In the Words of the Enemy," using statements by U.S. political and military leaders and prominent scholars to bolster the IS image. As an example, the first issue utilizes excerpts from a scholarly article written

---

[63] The idea of "Qisas" or retribution, is put forth in Koranic verse 16:126, though IS more regularly refers to the idea of mumathala. Terrence McCoy and Adam Taylor, "Islamic State says immolation was justified, Islamic Scholars say no," *The Washington Post online*, February 4, 2015, http://www.washingtonpost.com/news/morning-mix/wp/2015/02/04/the-chilling-reason-the-islamic-state-burned-a-jordanian-pilot-alive/ , (Accessed February 22, 2015).

[64] Duncan Gardham and John Hall, "Was Jordanian Pilot Burned Alive."

[65] Ibid.

[66] Hassan Hassan, "ISIS has reached new depths of depravity. But there is a brutal logic behind it," *The Guardian online*, February 7, 2015, http://www.theguardian.com/world/2015/feb/08/isis-islamic-state-ideology-sharia-syria-iraq-jordan-pilot , (accessed February 8, 2015).

[67] Ibid.

[68] In addition to English, versions are also available in Arabic, Russian, French, and German.

by prominent policy analysts Douglas Olivant, former Director for Iraq at the U.S. National Security Council, and Brian Fishman, former Research Director at the U.S. Combating Terrorism Center at West Point, who are both identified by those descriptors in the article. IS highlights the statements: "ISIS has created a multi-ethnic army; almost a foreign legion, to secure its territory" and "the group does not have safe haven within a state. It is a de facto state that is a safe haven."[69] Later issues incorporate quotes by President Barack Obama and former Secretary of Defense Chuck Hagel, among others. Taken collectively, the use of well-chosen public statements builds a case for the legitimacy of the Islamic State, demonstrating in effect, "look what our enemies say about us—we are real."

Every issue also includes scenes of battlefield victories, captured equipment and munitions, and smiling fighters working to help the newly loyal populace. They show scenes of communities being rebuilt, enemies being either punished or forgiven, and thieves and drug runners being brought to justice. Issue 5 announces a new mineral-based currency "in order to disentangle the [State] from the corrupt interest-based global financial system."[70] The topic is then reinforced in Issue 6 by an article from captured British war correspondent John Cantlie citing arguments about the impending collapse of dollar-based international markets from articles written by former U.S. Representative Ron Paul.[71] The clear message is that the steps the Islamic State is taking are *real and concrete*—that its money is made of gold or copper and has intrinsic value—versus an unsecured dollar standard. The Islamic State want readers to believe that the current world order is all a chimera, set to come crashing down, and the only place to find protection and relief from the ensuing chaos lies with the Islamic State.

While IS controls the content of *Dabiq*, it has far less control over internet forums that typically distribute the magazines. These forums are an open space in which news and information regarding jihad is exchanged. Photos, video clips, and audio excerpts, together with original articles and opinions, are traded freely along with news updates from various portions of the battlefield. In much the same way as Twitter users accrue followers, and thereby status, so too do those posting material to jihadist web forums gain status by "likes" and "shares" of their content.[72] Accrual of certain point levels moves one's postings to a different status, seen by more people and displayed more prominently.[73] As with any media forum, sensationalism is rewarded, and the more radical the author, the more likely (s)he is to gain a following. At the highest levels, one can even be rewarded with administrator status, or be given direct e-mail contact with key jihadist leaders, although reaching such levels requires years of jihadist study and near-constant dedication to the forums.[74]

More recently, IS forums contained video productions featuring John Cantlie together with scenes and graphics straight out of "Call of Duty," resulting in comments such as, "This is our Call of Duty and we respawn in Jannah (heaven)."[75] In other locations, forums feature legitimate video games parroting the gameplay of Grand Theft Auto, with an IS fighter performing all manner of incredible military acts to the accompaniment of jihadist music.[76]

Repetition of key themes is important for persuading potential recruits to take the step of traveling to the Islamic State, or to act on their own against the "enemies of Islam" wherever they may live. As IS becomes larger and more successful, keeping messages consistent and under central

---

[69] Douglas Olivant and Brian Fishman, "The Reality of the Islamic State in Iraq and Syria," as quoted in *Dabiq: Issue 1*, 32-33.
[70] Author not given, "The Currency of the Khilafah," *Dabiq: Issue 5*, 18.
[71] John Cantlie, "Meltdown," *Dabiq: Issue 6 – Al-Qaeda of Waziristan*, 61.
[72] Jarret Brachman and Alix Levine, "The World of Holy Warcraft."
[73] Ibid.
[74] Ibid.
[75] Terrence McCoy, "The Islamic State's 'Call of Duty' Allure."
[76] Ibid.

control may become increasingly difficult. IS leadership, through its official media organizations, creates and distributes solid products supportive of its cause and unified around consistent themes. The potential access of every group member to the internet, however, jeopardizes overall messaging as the organization becomes accountable for any messages or footage posted to the web in its name.

Highlighting the dangers of such communications access, throughout January 2015 various Twitter accounts regularly released execution videos and comments regarding the fate of Western captives that appeared to contradict leadership statements and lead to significant confusion.[77] In the days preceding the release of the al-Kasaesbah execution video in early February 2015, this mounting confusion was punctuated by the appearance of Caliph Ibrahim in a short online video with spokesman Mohammed al-Adnani clarifying that only four Twitter accounts were authorized to speak on behalf of IS—clearly, an effort to retain or regain control of organizational messaging.[78]

Millenarian Social Movement or Opportunistic Terrorism?

The purpose of this analysis has been to distinguish the Islamic State from its competitors in the Jihadist—and more broadly terrorist—realms. Rather than being directed and guided by a command structure, it appears that the low-technology Jihadist attacks occurring throughout 2014 outside of the Middle East and claimed by IS, were instead inspired by its message.

> O crusaders, you have realized the threat of the Islamic State, but you have not become aware of the cure, because there is no cure. If you fight it, it becomes stronger and tougher. If you leave it alone, it grows and expands.[79]

For Muslim youth, IS provides order and sanctuary from apparent chaos and an opportunity to resurrect the glory of the early Islamic Empire. IS pushes the message that death in the service of jihad is worth 60 years of prayer[80] and "saves 70 family members who were destined to go to the fires of hell.[81]" Death in Jihad offers immediate salvation for those with an imperfect—or criminal—past.

The most consistently identified factor responsible for militant religious violence lies with an individual's yearning for order and a sense of belonging. For non-Muslims searching for a way to lash out against the anomie of the modern world, unsatisfied with the surfeit of choices and potential possibilities of failure ahead, Jihad is the leading anti-western movement. Reasons for taking up arms in Jihad vary tremendously, however. Many young IS soldiers are likely fighting for reasons more closely akin to nationalism than religion, yet they go along with the organizational leadership, aping their statements and actions, in order to remain part of the group. Such differences in the commitment to and understanding of the doctrines involved likely result in internal conflict. *Dabiq: Issue 6* lectures IS soldiers and officials to follow orders and to moderate their behavior toward the

---

[77] Catherine Herridge, "ISIS Leader Warns Unauthorized Tweets Don't Speak for Caliphate," *FOXNEWS online*, February 2, 2015, http://www.foxnews.com/world/2015/02/02/listen-to-me-isis-leader-warns-unauthorized-tweets-don't-speak-for-caliphate/ , (Accessed February 8, 2015).

[78] Ibid.

[79] Abu-Muhammed al-Adnani al-Shami, "Indeed Your Lord is Ever Watchful," Arabic-language Audio Message posted to Hanin Network Forums by Al-Furqan Establishment for Media Production (dated September 21, 2014), Translation by al-Furqan, and posted by OSIS.gov as TRR2014092201178788.

[80] Jeffrey B. Cozzens, "Victory from the Prism of Jihadi Culture," *Joint Force Quarterly*, 52 (1st Quarter 2009): 88. http://ndupress.ndu.edu/portals/68/Documents/jfq/jfq-52.pdf (Accessed January 27, 2015).

[81] Jeffrey B. Cozzens, "Approaching Al-Qaeda's Warfare: Function, Culture, and Grand Strategy," (Draft) in *Mapping Terrorism Research*, ed. Magnus Ranstorp (London: Routledge, 2006), received directly from the author via e-mail and cited as page 16 of Chapter 7, within the larger work.

public. Such admonishment came just weeks before reports of infighting and large-scale desertions following battlefield setbacks in both Kobane, Syria and Ninevah, Iraq.[82]

In the fight against IS, the United States and its allies face two challenges: 1) defeating a semi-functioning outlaw state with a moderate military capacity, and 2) defeating a spiritual ideology. The Islamic State will face ever-growing challenges brought about by the sheer weight of governance as time passes. Its ability to sustain itself without formal sources of income is suspect, as its black-market sources are unlikely to suffice without additional resources acquired through conquest. Military stalemate and growth of governance responsibilities brings the added friction of simple boredom, which can be devastating to the revolutionary spirit necessary to sustain progress and development.

Jihad as espoused by Sayyid Qutb and embraced by IS provides an appealing anti-Western message that lends purpose to the lives of the susceptible. Scripture-based defenses against negative media portrayals already exist: "If your people fight you, accuse you of the worst of accusations, and describe you with the worst of all traits, then know that the people of the Prophet fought him, expelled him, and accused him with matters worse. . . ."[83] Though this is an ideology based on Islam, it is, however, a version of the religion most akin to a cult, defined by Colin Campbell as a "parallel religious tradition of disparaged and deviant interpretations and practices that challenge the authority of prevailing religions with rival claims to truth."[84] The idea that IS follows a deviant or discredited interpretation of Islam presents the biggest opportunity to effectively counter the ideology of the Islamic State.

The Islamic State is now a big organization, is continuing to grow, and, some estimates allege, has more foreign fighters today than were in Afghanistan at the height of the war against the Russians.[85] Almost all of the fighters can and do link to the internet via smartphones. Many statements and videos attributed to IS are apparently not being released and sanctioned by its central authorities. Instead, they likely originate from young fighters and commanders wanting to show how shocking or terrifying they can be. Such actions drive the admonishments and instructions IS published in *Dabiq* and via online videos in 2015. Violence without support of religious justifications damages IS legitimacy and standing among aspirants. Anything eroding the appearance of unity and moral certitude reduces the appeal of the organization to those recruits searching for the very same as an escape from their present lives. Likewise, failure to govern effectively or signs of infighting and desertion prove unhelpful and are likely to be prominently featured on major networks.

As with any cult, some people joining IS will discover that the group does not live up to expectations and they will seek to leave. Just as people can be "de-programmed" from cults, so too many can be "de-radicalized" from IS. Many young fighters are attracted by the adventure and the danger. They simply do not understand nor fully recognize what all that they are buying into, and they need an exit strategy, i.e., a way out. The way out, however, should be through government authorities and well-founded coordinated programs of counter-radicalization consisting of *prevention* up front and *de-radicalization* for those who initially decided upon jihad.[86]

When Islam first emerged in the Arabian heartland, the major empires of the day, the Romans and the Sassanids (Persians), had exhausted themselves from years of regional warfare. Rome had withdrawn from the Levant and placed in their stead puppet Arab rulers to keep the peace. Persian

---

[82] Tim Lister, "For ISIS, Tough Times as it Seeks to Regroup," *CNN online*, January 28, 2015, http://edition.cnn.com/2015/01/28/opinion/lister-bad-month-for-isis/index.html, (Accessed January 28, 2015), 4.

[83] Abu-Muhammed al-Shami, "Indeed Your Lord is Ever Watchful."

[84] Colin Campbell as quoted in Jeffrey B. Cozzens, "Approaching Al-Qaeda's Warfare," 2.

[85] Peter R. Neumann, "Foreign Fighter Total in Syria/Iraq now exceeds 20,000."

[86] Jessica Stern, "Deradicalization or Disengagement of Terrorists: Is it Possible?" in *Future Challenges in National Security and Law*, ed. By Peter Berkowitz, http://www.futurechallengesessays.com, (Accessed February 8, 2015), 1.

forces remained a threat both from the east and the south, where they ruled over Yemen. During this time of chaos for the Arab people, Mohammed emerged as a messenger from God, bringing order, purpose, and fraternity. The result exploded across the world with lightning speed and formed the basis of the Islamic Empire. That situation is not dissimilar to today, and IS knows it. By drawing upon the same elements today that existed during the time of the Prophet, IS believes it can completely redefine the social order and very nature of government through revolutionary violence to bring about a perfect society. That is, in short, not "simply" terrorism, but rather evidence of a millenarian social movement with an organized, developed plan to reorder the world.

Making a shift to conceive of IS as a millenarian mass movement is more important than it may initially appear. Military defeat of the group is absolutely important, but somewhat secondary to discrediting the ideology. The Islamic State is not random: though its message deviates from that accepted by mainstream Islam, it rests on core Islamic teachings and its grievances against the West enjoy broad-based support throughout much of the world. While time may eventually cause IS to collapse upon itself, the governments of the world would do better to cooperate in actively countering the ideology and the networks—both physical and cyber—that drive the group, while aggressively eliminating key leadership through all appropriate avenues. A failure to take the threat seriously, and as something much more than just a localized regional problem, may lead to a far bigger conflict than many security experts are inclined to think.

Army War College Review
Vol. 1, No. 3, Aug. 2015, 26-37

U.S. Army War College
Student Publications

The Flawed Strategic Discourse on Cyber Power

Brandon Newton

This paper examines flaws in the strategic discourse on cyber power. The current discourse is flawed because it is dominated by hyperbole, misapplies context, and lacks sufficient precision in terms and definitions. There are two critical flaws in the current discourse. The first is descriptions of the existential nature of strategic cyber war, and the Armageddon like environment that would be created by such a war, despite evidence to the contrary. The second flaw is in the understanding of the context of any cyber action initiated by potential adversaries, state or non-state. Recommended adjustments to the discourse need to be informed by clear and valid assumptions as to what can be done with cyber power, as well as crafting a model for cyber threat prioritization. The final analysis addresses both needed changes in education and training and human understanding of cyber power.

Keywords: *Cyber War, Cyber Strategy, Cyberspace*

If there were ever any doubt that cyber power had taken its permanent place among the more traditional domains of warfare, the recent National Security Strategy would erase that notion. According to the Strategy, cyberspace is the preeminent shared commons, an infrastructure responsible for our "economy, safety and health."[1] For the United States, cyberspace is an interest to be defended, with costs imposed on those who attack it. This year, 2015, marked a year of cyber events in the news and public debate, including the Sony Corporation hack, the Central Command Twitter hack, and assorted threats to financial networks.

Unfortunately, the hyperbole of a "Cyber 9/11" or "Cyber-Armageddon" has merged fact with fiction in the strategic discourse.[2] Although existing cyber-threats are certainly capable of striking U.S. interests, the likely effects of such attacks are being overblown and can be mitigated by current information assurance policies. After all, "Cyber war has yet to claim its first life."[3] In defense, business, and media circles, cyber threats are often presented as unqualified existential threats. The

---

Brandon Newton (M.S.S. United States Army War College) is a Colonel in the United States Army. *An earlier version of this article, written under the direction of Professor Thomas P. Galvin, earned a prestigious AWC Foundation Daniel M. Lewin Cyber-Terrorism Technology Writing Award for the class of 2015.*

[1] Barack H. Obama, *The 2015 National Security Strategy* (Washington, DC: The White House, 2015), 12.

[2] See Clifford S. Magee, "Awaiting Cyber 9/11," *Joint Force Quarterly* 70 (3rd Quarter, 2013).

[3] Martin Libicki, "The Nature of Strategic Instability in Cyberspace," *Brown Journal of World Affairs* 18, no. 1 (Fall/Winter 2011): 72.

current strategic discourse on cyber power and cyber defense is dominated by hyperbole, misapplies context, and lacks precision terms and definitions. The result is a flawed and incomplete development of policy and strategy for cyberspace and an unclear picture of how to interpret cyber threats strategically.

After clarifying relevant terminology and briefly reviewing current cyber power research, this essay exposes two critical flaws in the strategic discourse—overestimation of impact and lack of contextualization—that negatively influence both understanding of cyber power and our ability to mount an effective defense or response. The essay concludes by recommending new discursive strategies to more successfully navigate through the ever-changing cyber domain.

Terminology

Inconsistencies in use of cyber power terminology lead to confusion in the strategic discourse. This essay adopts Gray's approach to cyber terminology. Gray unpacks three terms: cyberspace, cyber power, and cyber strategy and provides useful definitions of each. *Cyberspace* is generally meant to describe the:

> Global domain within the information environment whose distinctive and unique character is framed by the use of electronics and electromagnetic spectrum to create, store, modify, exchange, and exploit information via independent and interconnected networks using information-communication technologies.[4]

Cyber power describes the "ability to do something strategically important in cyberspace."[5] Gray borrows from both Daniel Kuehl and air-power theorist Billy Mitchell in constructing this practical definition. The last term is *cyber strategy* (or as Gray puts it "strategies for cyber") and refers to explicit applications or designs for using cyber power in cyberspace. Gray emphasizes that "strategy is strategy, whether it is for cyber power, land power, or sea power."[6] His phrasing reinforces strategy as the prevailing concept *over* cyber—an essential step in emphasizing cyber powers' commonality with its sister domains, rather than primarily highlighting its technological distinctiveness.

The terms *cyber warfare* and *cyber war* are similarly important. Libicki provides an effective method of differentiating these two concepts. Cyber warfare describes the use of cyber power to accentuate warfare and combat in the physical domain. Cyber war describes cyber power used to affect the will of another nation or adversary.[7] In both cases, these terms describe warfare that takes place solely in cyberspace between adversaries seeking to use cyber power to affect another entity's will.

Current Research on Cyber Power

Compared with more traditional domains, a relatively small amount of research addresses the theoretical nature of cyber strategy and cyber power. Gray provides a few plausible reasons for this. According to Gray, what has been written is largely focused on the technical subject matter concerned with securing digital networks. Gray also notes that the strategic discourse on cyber was late in

---

[4] Daniel F. Kuehl, *Cyberpower and National Security*, ed. Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz, First edition. (Washington, DC: Center for Technology and National Security Policy ; National Defense University Press: Potomac Books, 2009), 28, quoted in Gray, *Making Strategic Sense* 9.

[5] Gray, *Making Strategic Sense*, 9.

[6] Ibid., 10.

[7] Martin C. Libicki, "Why Cyber War Will Not and Should Not Have Its Grand Strategist," *Strategic Studies Quarterly* 8, no. 1 (Spring 2014): 29.

coming because of a number of recent events: the so-called revolution in military affairs, transformation, and the post 9/11 war on terror.[8] The majority of what has been in the news and in the public discourse is that cyber warfare and cyber attacks are an existential and present danger to our national security. The best examples of strategic cyber warfare's effects can be found in articles like Amit Sharma's *Cyber Power, a Means to an End* and John Stone's *Cyber War Will Take Place!*[9] Numerous articles, books, and monographs portend a coming cyber war. Samples include *Awaiting Cyber 9/11* from *Joint Force Quarterly* and books and articles by Joel Brenner, such as *America the Vulnerable*.

A second and somewhat smaller community of scholars opposes the idea of strategic cyber warfare and the existential nature of the cyber threat. Libicki has written a number of expansive articles on cyber power including *Cyber Deterrence and Cyber War* and *Why Cyber Will Not and Should Not have its Grand Strategists*. Another important monograph is Gray's *Making Strategic Sense of Cyber Power: Why the Sky is Not Falling*. Both Libicki and Gray advance evidence and arguments consistent with the thesis of this essay. Other writers take a similar position, including Sean Lawson's *Beyond Cyber-Doom: Assessing the Limits of Hypothetical Scenarios in the Framing of Cyber-Threats* and a series by Thomas Rid including *Cyber War Will Not Take Place*. All persuasively minimize the existential nature of cyber power, and caution against overestimating the capabilities of cyber power and cyber warfare.

Problems with the Discourse

The current discourse is marred by two critical flaws. The first is the degree to which writers have extolled the existential nature of strategic cyber war, and the Armageddon like environment that would be created by such a war—despite impressive evidence to the contrary. Overestimating the capabilities of cyber warriors and effects of cyber warfare confuses the realities of what can be done with cyber power. It is certainly possible that cyber power alone could result in actual physical harm, but as of 2015 cyber attacks have only generated effects indirectly. Cyber warfare's ability to force a strategic reaction that affects the will of a nation is suspect, given that, according to Libicki, even a catastrophic loss of digital networking capability can be overcome. Imagining a scenario in which cyber power alone (promulgated through a cyber war) would pose an existential threat to the U.S. is difficult.[10] A properly shaped discourse recognizes how rapidly cyber threats are adapting and evolving, and can aid policy makers in properly aligning resources against the threats, while avoiding hyperbole in favor of a rational and suitable assessment of the real capabilities of cyber power.

The second flaw lies with understanding the context of any potential cyber action by state or non-state adversaries. The loss of sensitive company data by Sony in 2014 as a result of a North Korean cyber attack was certainly damaging to the Sony Corporation and shareholders. Absent, however, was vital contextualization of the hack with regard to both policy and strategic response. The losses seemed to result in real monetary damage to Sony, but what national interest was placed at risk? What was lost in the attack and whom did it affect? What were the North Koreans able to hold at risk that directly or potentially impacted U.S. national security? The corporation was coerced into removing *The Interview* from theaters and the U.S. threatened to "respond proportionality"

---

[8] Gray, *Making Strategic Sense*, 7.

[9] John Stone, "Cyber War *Will* Take Place!" *Journal of Strategic Studies* 36, no. 1 (February 2013): 101–108.

[10] Martin C. Libicki and Project Air Force, *Cyberdeterrence and Cyberwar* Online (Santa Monica, CA: RAND, 2009), 137, http://search.ebscohost.com/login.aspx?direct=true&scope=site&db=nlebk&db=nlabk&AN=304894 (accessed January 8, 2015).

against the North Koreans.[11] The judgment of *what matters and why* for an action taken in cyberspace is relevant and important. This examination should be more acute when the causal agent and attribution is to a state, especially when language that is normally reserved for actions in traditional domains is applied at the Executive level of the U.S. government.

Overestimating Strategic Cyber War

The current discourse of overestimation leads to evaluation of cyber war as an existential threat and a corresponding survival interest. Two examples drawn from Joel Brenner and Amit Sharma suffice. In *America the Vulnerable*, Brenner overestimates cyber power's impact and reach in warfare. He describes a hypothetical future (2017) cyber-enabled conflict between China and the U.S. The scenario culminates when the U.S. is coerced to acquiesce to China's demands in the South China Sea after China demonstrates the ability to control the U.S.' critical power infrastructure.[12] Gray argues that this type of strategic cyber war is infeasible. Cyber power "can only be an enabler of physical effort" and that "stand-alone (properly misnamed as 'strategic') cyber action is inherently and grossly limited in its immateriality."[13] The idea that strategic cyber warfare, executed singularly without the complementary effects of traditional air, space, sea, and land warfare characterizes cyber power as having a "specialness" that is simply inaccurate. Cyber power is fundamentally under the same constraining factors of the weapons and tools available in the other domains of war.[14]

In Sharma's (over)estimation, cyber power's place in warfare has been wrongly employed as an adjunct to traditional operations which he believes should enhance strategic cyber warfare, not the reverse. Sharma applies Clausewitz's trinity to cyber capabilities, envisioning the ability of cyber power to destroy all of the cyber-manifestations of the trinity, causing a cascading effect that will "induce a strategic paralytic effect on the nation, pushing it into chaos and mayhem."[15] According to Sharma, strategic cyber war's impact on the state is explained in existential terms, with the ability to affect basic national resilience. An attack on all aspects of the Sharma's cyber trinity (defense networks, government and law enforcement networks, and critical national infrastructure) would cripple the government and promote widespread chaos.

> The disappearance of their facilities on which they are hopelessly dependent will result in catastrophic outcomes, where chaos, fear, bedlam, anarchy, and basic animal instincts will prevail, resulting in complete destruction of the nation as a system.[16]

Yet, cyber warfare is unlikely to have the effects that Sharma portends. Should we experience a worst case scenario of cyber attacks on digital networks and systems, the nation simply returns to its pre-networked state. According to Libicki, "to argue that cyber warfare can have a revolutionary effect on the battlefield requires establishing that digital networking is itself revolutionary. This is a step many proponents of cyber warfare neglect to take."[17] This analysis does not discount the very real indirect effect that cyber can achieve, rather it informs the magnitude of the effects on all aspects of the government and life. Society possesses far more resiliency in the face of the type of adversity

---

[11] Barack H. Obama, "Remarks by the President in Year-End Press Conference Online," *The White House*, http://www.whitehouse.gov/node/314731 (accessed February 23, 2015).

[12] Joel Brenner, *America the Vulnerable: Inside the New Threat Matrix of Digital Espionage, Crime, and Warfare* (New York: Penguin Press, 2011), 137.

[13] Gray, *Making Strategic Sense*, 44.

[14] Ibid., 14.

[15] Amit Sharma, "Cyber Wars: A Paradigm Shift from Means to Ends," *Strategic Analysis* 34, no. 1 (January 2010): 64.

[16] Sharma, "Cyber Wars," 65.

[17] Libicki, "Why Cyber War," 29.

Sharma describes. Lawson questions the idea that cyber war could achieve this type of devastation, if massive conventional and atomic air attacks on populations "generally failed to deliver the panic, paralysis, technological and social collapse, and loss of will, it seems unlikely that a cyber-attack would achieve these results."[18] By comparing historic devastating attacks on the U.S. (e.g., a "cyber Pearl Harbor" or Cyber 9/11) with cyber warfare's potential impact, some authors capitalize on our knowledge of those events to illustrate a level of devastation that is familiar.[19]

The overestimation of cyber power is a continuance of a distrust of technology and a belief that computers could spin out of control and act independently. As such, the tendency to overestimate the threat continues to feed historical technological pessimism and fear of new innovations—a fear reinforced by our ever-present reliance on digital networks.[20] Comparisons to attacks like 9/11 or Pearl Harbor are suspect. In those attacks, the population was physically affected, but was certainly resilient enough to eventually recover and move forward. Any cyber exclusive attack is unlikely to have an impact *nearly* as devastating as recent large natural disasters or the strategic bombing campaigns of World War II.[21] An additional view on cyber doom scenarios is that we have already experienced that level of attack, but the damage was existential in other more broadly defined ways. In execution, cyber warfare may look less like earthquake and more like climate change; "[Snowden] is our Cyber 9/11, we just imagined it differently."[22]

Strategic cyber warfare is often credited with the ability to influence the will of an adversary and with capabilities as powerful as our most lethal strategic weapons. Sharma argues that cyber warfare can have an attractive outcome: conflict termination without conventional warfare, for example. He argues that strategic cyber warfare against the Trinity in order to achieve strategic paralysis is:

> eventually more important than the conventional paradigm of destruction-based warfare to annihilate the forces it depends on for its defence; generating not only a strategic victory, but also a constructive conflict termination.[23]

Sharma continues by making the linkage between constructive conflict terminations as a modern day requirement, strengthened by the domestic necessity of not repeating protracted conflicts like the Iraq War.[24] Gray's observation is that it would be difficult to extrapolate the ability of cyber power to cause enough kinetic damage to force a change of national will. He also notes that it is not hard to draw analogies with other non-kinetic methods and see that cyber could be included for its ability to have an indirect effect as well as a "contributing enabler of effectiveness of physical efforts in the other four geographies of conflict. Speculation about cyber war, defined strictly as hostile action by networked computers, is hugely unconvincing."[25]

Finally, two other explanations for this flaw in the discourse warrant consideration. The first is that this inflation is an example of securitization theory, which establishes that when threats to security are not "naturally occurring, they must be constructed through political and public discourse."[26] This unnatural elevation of cyber threats increases the funding, attention, and

---

[18] Sean Lawson, "Beyond Cyber-Doom: Assessing the Limits of Hypothetical Scenarios in the Framing of Cyber-Threats," *Journal of Information Technology & Politics* 10, no. 1 (January 2013): 45.

[19] Susan W. Brenner, *Cyberthreats and the Decline of the Nation-State* (Florence, KY: Routledge Research in Information Technology and E-Commerce Law, 2014), 71.

[20] Lawson, "Beyond Cyber-Doom," 90.

[21] Ibid., 95; Libicki, "Why Cyber War," 32.

[22] Thomas Rid, "Rid Replies," *Foreign Affairs* 93, no. 2 (April 3, 2014): 167–168.

[23] Sharma, "Cyber Wars," 67.

[24] Ibid.

[25] Gray, *Making Strategic Sense*, 45.

[26] Lawson, "Beyond Cyber-Doom," 88.

importance of the enterprise needed to defend against cyber threats. The other possibility is that cyber "catches the wave" of the public desire that gravitates towards defense solutions offering a technological standoff as opposed to boots on the ground (or in the air).[27] The discourse on cyber power and cyber strategies is often missing a critical assessment of what, realistically speaking, can be done in cyberspace and toward what end.

Context and Vulnerabilities in Cyberspace

Cyber power and cyber vulnerabilities need to be placed in strategic context and considered relative to other methods of warfare. The ease with which we apply strategic theory from other domains to cyber warfare hampers clear thought on what cyber power can and cannot do. Some hampering can be attributed to the immaturity of what we know about cyber power's possibilities, and in many cases we simply do not yet know "enough now to make strategic sense of cyber."[28]

In November 2014, The Sony Corporation's network was penetrated by what was reported to have been North Korean cyber-units. The intrusion acquired a large amount of corporate and personal data, emails, and business intelligence. Analyzing the Sony attack provides useful insight with regard to context and vulnerabilities.

The stated U.S. national reaction to "respond proportionately" to the North Korean use of cyber-power against Sony, underwrote a policy to act with cyber power even when the adversary's objectives were not achieved.[29] The affected movie, *The Interview*, was critically panned and anticipated to become a commercial flop, but became far more successful after the cyber-attack.[30] But what really caused that turnaround—was it the resilience of a media corporation or simply public reaction to widely spun national rhetoric? The concern for policy and strategy is that without proper context the strategic effects of cyber activity could be wrongly attributed. Incorrect attribution could easily lead to significant future vulnerabilities. Libicki urges caution:

> Strategic effects of cyber war may arise from the interaction of state actors that systematically overestimate its effects (as quasi-apocalyptic statements from both U.S. and Chinese military officials suggest is quite possible). This could lead to unfortunate dynamics.[31]

As it turned out, the exploitation of the Sony's network was not a sophisticated attack, and had more to do with poorly safeguarding sensitive (at least to them) data than it did with superior cyber power capabilities wielded by North Koreans.[32]

Another issue with national response absent context is that cyber power may be unique, but it is constrained by the same theoretical properties as the weapons of the other domains. Cyber power can achieve indirect effects against economies, information, and certainly defense forces, but they must be viewed carefully and in context of cyber power's place as a tool for furthering strategy. Gray points out that cyber may be an "extreme case of non-kinetic agency, but the legal problems (in the

---

[27] Gray, *Making Strategic Sense,* 6.

[28] Ibid., 4.

[29] Obama, "Remarks by the President"

[30] Ann Hornaday, "Review: 'The Interview' Has Some Laughs and Makes Some Points but Isn't as Edgy as Its Reputation Suggests Online," *The Washington Post*, December 24, 2014, http://www.washingtonpost.com/lifestyle/style/review-the-interview-has-some-laughs-and-makes-some-points-but-isnt-as-edgy-as-its-reputation-suggests/2014/12/24/97b85a8a-8ba9-11e4-a085-34e9b9f09a58_story.html (accessed March 22, 2015).

[31] Libicki, "Why Cyber War, Strategist." 33.

[32] ScienceFriday, "Which Cyber Hacks Should We Worry About?" January 16, 2015, *Science Friday.com*, streaming video, 12:23, http://sciencefriday.com/segment/01/16/2015/which-cyber-hacks-should-we-worry-about.html (accessed January 23, 2015).

laws of war) created by regarding combat electrons effectively as equivalents to agents of force ought to be overwhelmed by strategic sense."[33] The Sony hack is a good example of phenomena described by Peter Singer: "Essential concepts that define what is possible and proper are being missed, or even worse, distorted."[34] This causes "past myth and future hype" to combine, making what actually happened even more difficult to discern.[35] The conclusion is that the context of cyber power and strategy is important, as well as careful consideration of what makes our cyberspace vulnerable.

Vulnerabilities in cyberspace are variable, and often the result of a need for individual convenience and profit for business. In 2015, government, business, and private citizens have a reliance on digital networking that is not only a matter of convenience, but, in some cases, is required by law. The current trend toward increased digitization is unchecked and not likely to change. What should not be lost in the discourse, however, is that in cyberspaces an absolute separation exists between what can occur in those constructed spaces and what is truly a vulnerability. As Valeriano and Maness explain:

> The most important distinction of cyber is that between the physical and synaptic layer. These layers are not collapsed together. The danger coming from cyber invasions can only apply to the knowledge existing in the information world and not to all knowledge. In other words the state is only as vulnerable at it allows itself to be.[36]

Jeffery Carr articulates the misplaced context of cyber when stating "the potential effect of a digital or cyber weapon used against a network is directly proportional to how much a given population relies on that network."[37] Exploitation of a corporate or defense network is not a random event that just occurs on its own. Carr offers a powerful and realistic counter argument that should not be minimized in a discussion of cyber power's real capabilities. Framing the impact of a cyber event as a constant and sustained vulnerability ignores the reality that we can be proactive in adjusting our posture once attacked. This goes farther than the ideas of improved defensive positions. In a constructed space, a space that is inherently virtual, choices and adjustments can be made with regard to reliance on the medium. The irony with cyberspace is that its physical properties may be non-permissive, but it facilitates the construction of very permissive and discretionary environments, altered and adjusted by the user of the space.[38]

Analyzing Cyber Power and the Strategic Context

Embracing flawed assumptions about cyber power has negative implications for cyber policy. Assumptions that overestimate cyber power, as has been illustrated, is risky and ill advised. Focusing policy on the least likely scenarios of so-called cyber-warfare diverts resources away from "preventing or mitigating the effects of more realistic but less dramatic scenarios" that are actually more likely to be encountered.[39] Recent focus has been about loss of data and hacks by state actors against both government and business. Data hacks prompted calls for government reaction, primarily defense.

---

[33] Gray, *Making Strategic Sense,* 14.

[34] P. W. Singer, *Cybersecurity and Cyberwar: What Everyone Needs to Know* (New York: Oxford University Press, 2014), 6.

[35] Ibid.

[36] Brandon Valeriano and Ryan Maness, "Persistent Enemies and Cyberwar" in *Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World*, ed. Derek S. Reveron (Washington, DC: Georgetown University Press, 2012), 141.

[37] J. Carr, "The Misunderstood Acronym: Why Cyber Weapons Aren't WMD," *Bulletin of the Atomic Scientists* 69, no. 5 (September 1, 2013): 32.

[38] Ibid., 39.

[39] Lawson, "Beyond Cyber-Doom," 96.

What we have, however, if properly understood, are opportunities for more clearly understanding the role of national policy and defense in responding to the cyber power needs of non-defense entities. Following the economic crisis of 2008, many financial companies acknowledged that they had contributed to the mistakes directly resulting in the crisis and the subsequent regulation. Interestingly, however, they do not appear to share that same feeling of culpability for failing to secure their networks and data, and rather see a role for government protection and defense involvement.

The discourse needs to always strive for clear problem definition in assessing cyber power and cyberspace. Lawson's example is to disaggregate the threats, and "focus on broader range of cyberspace-based events, e.g., human error, market failure, technical failure, in addition to malicious attacks by actors with intent to disrupt."[40] In other words, the focus of some strategic thought on massive cyber war and the effort that goes into preparing to defend against that unlikely event can mask the nature of other less-obvious cyber threats with the potential for real strategic impacts. Edward Snowden's global (and illegal) publication of sensitive national security and diplomatic information is an example of more broadly defining the threat. His actions did real strategic damage to our diplomatic, informational and defense power in a way that exemplifies the existential cyber war for which the U.S. has been preparing.

The discourse also needs to center more around empirical research and less on hypothetical scenarios when evaluating what is in the realm of the possible in cyberspace.[41] Defense techniques that incorporate operational design can be helpful in framing the environment as well as the problem definition. Those charged with policy and strategy decisions about cyber power should demand a level of accuracy in information and problem framing that relies on far more than inductive anecdote. Lack of unfamiliarity with technology cannot be an impediment to understanding the nature of cyber power and good decision making. Strategic leaders must be quick to question and critically analyze whether what they are hearing is "based on empirical evidence or merely the reflection of long held anxieties about technology and recycled assumptions about infrastructure and social fragility."[42]

Finally, the discourse needs to shift its outcomes away from a crisis response orientation and toward developing ways and means that promote resilience in technological and social systems that ultimately bound cyber power and cyberspace. As the several examples indicate, the cyber domain is constructed and is largely what its users make of it. Lawson calls for three initiatives:

1. modernization and repair of infrastructure,
2. promoting strong local communities and good governance, and
3. increasing decentralization and self-organization in social systems.[43]

Defense strategy concerned with cyber power can improve most by increasing decentralization. That this imperative includes decentralization as a way to form cyber policy is unique. This idea should be familiar to military leaders due to parallels with principles within Mission Command doctrine.

A Model for Assessing Cyber Threats

The Carnegie Mellon Software Engineering Institute proposes a useful holistic model for understanding cyber threats. The Cyber Prioritization Model (CTP) was a result of a larger study on cyber intelligence across business, government, and industry. During the study the research team noted diverse and problematic methods that were used to prioritize and understand various cyber

---

[40] Ibid., 97.
[41] Ibid.
[42] Ibid.
[43] Ibid.

threats.[44] When applied to problems of defense and strategy, this model could assist in better framing the strategic context of cyberspace threats.

The model disaggregates threats into three areas for analysis: (1) the *likelihood* of threat actors executing attacks, (2) the *impact* that the threat could have on the organization, and (3) the *risk* a threat poses based on an organization's known vulnerabilities.[45] The cyber threat prioritization model is helpful for thinking strategically about cyber power and cyber strategies, sorting through threats, and identifying or prioritizing threats in terms familiar to defense leaders. The model is based on a summation of likelihood, impact, and risk. Likelihood is a function of understanding the capability and intent of cyber threat or actor. Attack methods, resources, motive and targeted data are all a part of analyzing and qualifying likelihood.[46] Impact is about assessing effects. In the CTP model, impacts are grouped into two areas: operational impact and strategic interests.

The CTP model does not wholly omit the nature of national security impacts and interests, but considering the strategic impact of systems related to homeland security and defense is necessary. The third portion of the CTP model deals with risk. This component is also useful for thinking about DoD vulnerabilities. The CTP model identifies two categories of risk: people and the cyber-footprint.[47] What is interesting about the risk dimensions of the CTP model is the assumption that vulnerabilities are dependent on the organization's choices and the people in that organization—an assumption in keeping with earlier discussions on discretionary vulnerability. The results of the three-part analysis can then be plotted on a graph similar to Figure 1. Analyzing potential cyber threats using this these modeled areas is helpful to understanding threats based on discreet characteristics. Doing so facilitates aligning the policy and prioritization of limited resources for the organization's cyber efforts.[48]

How does this holistically apply to understating cyber threats with national security implications? By seeing threats parsed among these three areas and evaluating them separately, we can make informed decisions on strategy and policy. For example, in Figure 1, the *impact* of the disruption of networks and systems that control the nation's nuclear arsenal would occupy the "high" quadrant. This should lead to a corresponding understanding that our cyber strategies in the *risk* quadrant must reduce the cyber footprint (e.g., network and digital reliance) while reducing opportunities for human error and interaction with digital networks. Libicki (also quoted in Gray) provides a concise example:

> There is no inherent reason that improving information technologies should lead to a rise in the amount of critical information in existence (for example, the names of every secret agent). Really critical information should never see a computer; if its sees a computer, it should not be one that is networked; and if the computer is networked, it should be air gapped.[49]

---

[44] Jay McAllister and Troy Townsend, "Implementation Framework- Cyber Threat Prioritization Online," *Carnegie Mellon University Software Engineering Institute* (September, 2013): 4.3, http://sei.cmu.edu/about/organization/etc/upload/framework-cyber.pdf (accessed March 6, 2015).

[45] Ibid.

[46] Ibid., 4.6.

[47] Ibid., 4.8.

[48] Ibid., 4.3.

[49] Martin C. Libicki, *Conquest in Cyberspace: National Security and Information Warfare* (New York: Cambridge University Press, 2007), 105-106; Martin C. Libicki and Project Air Force (U.S.), *Cyberdeterrence and Cyberwar Online* (Santa Monica, CA: RAND, 2009), 19, http://search.ebscohost.com/login.aspx?direct=true&scope=site&db=nlebk&db=nlabk&AN=304894 (accessed January 8, 2015); quoted in Gray, *Making Strategic Sense*, 47.

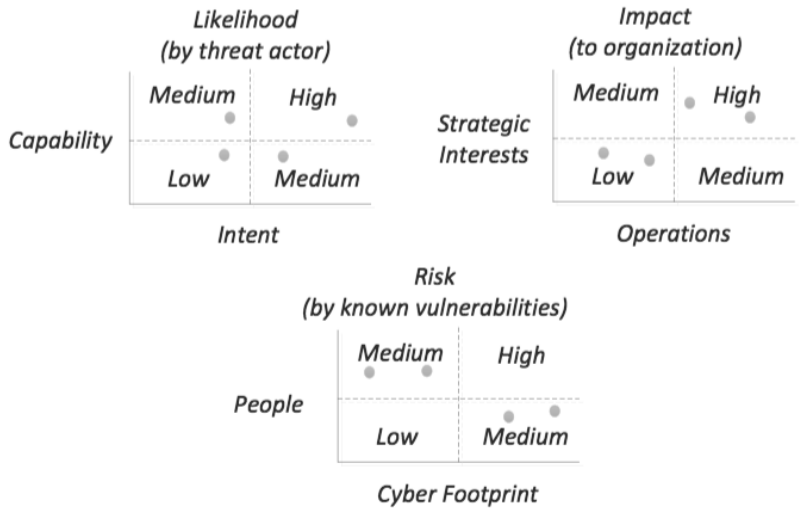


Figure 1. Cyber Threat Prioritization Model[50]

Assessment of impact and likelihood can effectively inform prioritization of effort and help to reduce risk. The distinction in both examples is that the vulnerability is discretionary. People, the cyber footprint, and the resiliency of the systems (both digitally and socially) are all adjustable and malleable. They also exist astride the digital domain and the human domain.

Our reliance on digital networking will not be reduced as time and technology increase capacity and capability. Of interest are the nature and characteristics of cyberspace as they relate to strategy. Participation in cyberspace is discretionary. The human beings who construct cyberspaces and reconstruct them rapidly define vulnerabilities and opportunities. When approached strategically, "Cyberspace can be what we and our enemies make of it."[51] Users participate in their own exposure in cyberspace in a unique way compared to the other traditional domains.

Recommendations

The final analysis of the cyber power conversation begins with what our role is with regard to learning about cyber, understanding vulnerabilities, and perceiving risk. The policy and strategy documents that lay out the direction for operating in cyberspace are misaligned with the actions that the U.S. is taking to understand the primacy of humans in this domain. Humans ultimately are responsible for making judgments on context, vulnerabilities, and the strategic significance of cyber power. In spite of policy statements establishing the need for a cyber savvy workforce and defense strategies that call for better "cyber-hygiene," most of the effort has been on the technical aspects of securing digital networks and developing new command structures for managing cyber forces.[52] People, however, are ultimately the arbiters of collective success in cyberspace.

One example of the primacy of people and cyber is the 2011 DoD Strategy for Operating in Cyberspace that emphasizes people as the first line of cyberspace defense. It directs the "fostering of a culture of information assurance" and advocates high costs for those who engage in malicious

---

[50] Ibid., 4.4.
[51] Ibid., 31.
[52] *Department of Defense Strategy for Operating in Cyberpace*, 6.

activities from inside the network.[53] A cultural shift would be enabled by "new policies, new methods of personnel training, and innovative workforce communications."[54] This innovation in training and culture has not gained noticeable traction since the publication of the document. The DoD must increase the education of users and leaders across the board, not just in those specialties related to digital networking.

Education is a baseline for understanding cyber power's real capabilities and context. The general choice to remain uninformed and uneducated about the true nature of cyber power has diluted both the discussion and understanding of risk. By remaining relatively uninformed about what is possible, people become disassociated and divested from the outcomes. Even if strategic cyber warfare is unlikely, cyber power as a complementary action to operational warfare is a reality, and the cyberspaces in which all operate are ubiquitous. What is not ubiquitous, however, is a common familiarity with those tools, their capabilities, and an understanding of what is actually possible in cyberspace. As noted above, a common thread in the strategic literature places people as the front-line of defense in cyberspace. What remains in practice, however, is a focus on minimizing the responsibility of users and leaders, hardening our systems, and specialization of expert knowledge. For the U.S. Army, the majority of users' cyber responsibility is simply answering a question (right or wrong) on a logon screen and taking an annual class on information assurance. This minimalist approach to education on cyber power and cyberspace relies primarily on centralization and control.

Operations in cyberspace and reliance on digital networking are a given. Cyber power-enabled intelligence can be a significant weapon to complement operational warfare, and can be a threat when wielded by a well-resourced adversary. In practice, the DoD should demand as much understanding of this weapon as with any other individual weapon. One could not imagine dissociation with a pistol or rifle that was as diluted as current individual knowledge about cyberspace and digital networks. Daily interaction with digital networking is exponentially more frequent than with an M4 carbine or M9 pistol, yet there is a considerable amount of dissociation with the former that is not tolerated with the latter.

Policy that focuses on the technical aspects of threats and risk reduction at the expense of education and training may be less useful as technology further evolves. Kraft, et al., called this the "Adam and Eve Paradox," whereby in spite of the Moore's Law and the exponential improvement in technology every 18-24 months, the slant of cyber attacks and threats is trending towards less sophisticated attacks that target "low hanging fruit," defined as targets that typically involve human mistake and weakness.[55] The paradox is that as technology gets more capable, so do the technical mechanisms to reduce risk. In the cyber threat priority model above, this would translate into having the ability to affect the cyber footprint positively at the pace in which technology and the threats advance. The result is that risk is now more skewed towards the low hanging fruit (i.e., *the people* in our organizations). Thus, the military ought not choose to minimize education, but rather must expand the knowledge and responsibilities about cyber power across all of its units and activities. The cyber specialization of units and occupational specialties is necessary, but should be

---

[53] Ibid., 7.

[54] Ibid.

[55] Moore's Law is the observation by Gordon E. Moore that over the history and glide path of computing hardware, the number of transistors that can be placed within an integrated circuit doubles every two years. This concept is explained in detail in Moore's paper "Cramming More Components onto Integrated Circuits," *Readings in computer architecture* (2000): 56, and the online source "Moore's Law, Part 1: Brief History of Moore's Law and Current State," *Research Blog*, n.d., http://googleresearch.blogspot.com/2013/11/moores-law-part-1-brief-history-of.html (accessed March 25, 2015); Michael Kraft, et al., "The Adam and Eve Paradox," Proceedings of the International Conference on Information Warfare & Security, January 2013, 275.

accompanied by robust programs to educate the majority of cyberspace participants in order to build needed resiliency within the larger network.

Lawson warns against users of cyberspace being passive consumers, lacking the digital skills and understanding necessary to overcome adversity should a disruption occur.[56] DoD policy makers should take this into account when developing units and systems that minimize user involvement. Patrick Jogoda describes solutions to cyber challenges with a similar idea of decentralization. The best solutions for defending cyberspace and responding to attacks will not come from promoting centralized and monolithic structures but will be "more Wikipedia than Manhattan project. It takes networks to understand, manage, and build networks. In the early 21st century, total control—however well-intentioned—is a fantasy."[57] The trade off in controlling systems and users while decentralizing network power must be carefully balanced in a defense setting.

Conclusion

Cyberspace is a finite domain, bounded at least for now by the physical properties of voltage, and the mathematical properties of logical sequences and combinations.[58] In the end we *choose* to avail ourselves of the benefits of cyberspace, and "if that cyberspace is found vulnerable to attack, or unexpectedly prone to technical failure, the fault will be ours."[59] Yet, the strategic discourse on cyber power overestimates the threat and minimizes the context while reducing the breadth of education and understanding by the human element. The premise that gives existential capacity for cyber to damage our security interests, and then applies the theories of other traditional domains, fails to acknowledge the constructed and participatory nature of cyberspace. Moving beyond flawed assumptions for cyber power and cyber strategy will enable strategic leaders to analyze threats based on their likelihood, impact, and risk and consequently enable a more effective response.

---

[56] Lawson, "Beyond Cyber-Doom," 98.

[57] Patrick Jogoda, "Speculative Security," in *Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World*, ed. Derek S. Reveron, (Washington, DC: Georgetown University Press, 2012), 33.

[58] Technical Singularity is the prediction or hypothesis by Victor Vinge that the continued advances in technology will lead to a change that is comparable to the rise of human life on Earth. Vinge presented in this idea in 1993 at a NASA symposium and in a paper titled *The Coming Technological Singularity: How to Survive in a Post-Human Era*. At the time he predicted that within 30 years the technological means to create superhuman intelligence would emerge, thus ending the human era. A wealth of current research on singularity blends artificial intelligence, biology, and religion; see B. R. Bannister, *Fundamentals of Modern Digital Systems*, 2nd ed. (New York: Springer-Verlag, 1987), 1.

[59] Colin S. Gray, *Making Strategic Sense of Cyber Power: Why the Sky Is Not Falling* Online (Carlisle, PA: Strategic Studies Institute and U.S. Army War College Press, 2013), 39, http://www.strategicstudiesinstitute.army.mil/pubs/display.cfm?pubID=1147 (accessed February 23, 2015).

Army War College Review
Vol. 1, No. 3, Aug. 2015, 38-41

U.S. Army War College
Student Publications

Moving to the City

Andrew M. Zacherl

The terror attack of September 11, 2001—one of the most profound and world changing events of the past sixty years—continues to impact the world's political, military, and economic environments. Yet world environments are shaped as much by ongoing processes as by traumatic events. Subtle and ongoing forces significantly alter both the conduct of military operations and the strategies utilized to pursue and protect each nation's interests. Urbanization of the world's growing population and rapid expansion of information and communication technologies (ICTs) are prime concerns.

Urbanization has generated complex urban environments that are larger in population and physical size than at any time in human history. These megacity environments serve as homes to a vast diversity of ethnic, cultural, and economic groups and are the primary conduits for resources flowing into and out of surrounding rural areas.[1] The percentage of people residing in urban areas has continued to increase since the industrial revolution. In 1800, only 2% of the world's population was urbanized; in 1950 that number had climbed to 30%; and by 2000, 47% of the world's population were urban dwellers.[2] This concentration of humanity, resources, and critical infrastructure drastically impacts the environment in which international competition and conflicts occur. Moreover, this trend is most pronounced in areas of the developing world which, due to a lack of financial resources, modest managerial capability, and uneven political will, are governed by entities "least equipped to handle" massive urbanization.[3]

Information interconnectivity, likewise, has expanded exponentially through the growth of information and communication technologies. As people worldwide become more connected through technology, their social environments potentially expand from the local to the global level, and their ability to convey information and exert influence becomes more pronounced. The ability to transmit and receive information makes every connected person a potential conflict participant whether through observation, indirect involvement, or direct contribution.

The strategies a nation must employ to achieve or protect its national interests must account for these increasingly important forces. For the United States, maintaining strategic legitimacy and credibility[4] when military force is employed requires commitment to the Law of Armed Conflict and

---

Andrew M. Zacherl (MMAS Air University) is a Colonel in the United States Army. An earlier version of this article was written while the author was a United States Army War College Fellow at Tufts University.

[1] David J. Kilcullen, *Out of the Mountains: The Coming of the Urban Guerrilla* (New York: Oxford University Press, 2013), 42.

[2] United Nations Habitat Organization. "Urbanization: Facts and Figures" http://ww2.unhabitat.org/mediacentre/documents/backgrounder5.doc (accessed October 28, 2014).

[3] Kilcullen, *Out of the Mountains*, 28.

[4] James D. Campbell, "French Algeria and British Northern Ireland: Legitimacy and the Rule of Law in Low-Intensity Conflict," March-April 2005, http://www.leavenworth.army.mil/milrev/download/English/MarApr05/campbell.pdf (accessed October 28, 2014).

to the principles of discrimination[5] and proportionality.[6] The "cluttered" nature of urbanized terrain where combatant, non-combatant, and critical infrastructures are tightly packed in close proximity makes adherence to these principles particularly challenging.[7] Discrimination:

> ensures that we aim only at the right target at the right time. In complex urban terrain there is a constant risk of striking innocent civilians, or destroying infrastructure of cultural or political significance. Our enemies deliberately seek to provoke an over-reaction from us in the presence of innocent civilians. This is a clever use of asymmetry against our greater firepower . . . Nothing undermines the credibility of our efforts more than the unintended killing of civilians.[8]

The consequences of errors in discrimination or missteps in proportionality are magnified by the proliferation and use of information and communication technologies. The battle at the Qasr al-Nil Bridge on January 28, 2011 during the Egyptian uprisings against the Mubarak regime exemplifies this reality. During the battle, protestors marching to Tahrir Square faced off against Egyptian security forces who, in turn, utilized particularly brutal riot control tactics during the confrontation. The ferocious street battle assumed strategic importance through an exceedingly effective media campaign strategy that fully leveraged modern ICT capability. The protest elements used mobile phone video posted to YouTube to document and disseminate the regime's brutality and the protestor's solidarity and resolve. Kilcullen describes the effects of this violent confrontation and the following media action as one of "the most pivotal battles of the revolution."[9] Taken together, urbanization and ICT proliferation create a challenging situation demanding an appropriate strategy for military engagement in large urban environments.

Despite dangers and pitfalls, avoiding urban environments altogether is unlikely, unrealistic, and significantly overlooks an opportunity. Modern urbanized areas provide unique cross-domain access making them strategic decisive points. Complex urban environments are the intersections of land, sea (where applicable), and information connectedness/cyber domains.[10] Strategic benefits inherent in maintaining control of the assets of a modern urban environment include: access to the littorals and air/sea port facilities therein, control of telecommunications and cellular network hubs, and direct access to large population segments in a concentrated area. Whether from a pure access or a population-centric examination, urban environments clearly serve as decisive points in the modern world. Furthermore, they can only be effectively leveraged through the application of capabilities residing in the physical domain: the land domain which offers direct and persistent access to these environments.[11] At the same time, however, the capabilities employed within the land domain must be applied appropriately to account for the human response to operations in urban environments. Application of inappropriate means in the execution of a given strategy damages legitimacy and outweighs any potential benefit gained by controlling an urban area. To achieve Landpower's true strategic potential, a full suite of land-based capabilities must be advanced to

---

[5] The principle of discrimination requires distinguishing between combatants, who may be attacked, and noncombatants, against whom an intentional attack may not be directed, and between legitimate military targets and civilian objects. This definition is derived from the 1991 U.S. Department of Defense final report on the conduct of the Gulf War.

[6] The principle of proportionality requires that the anticipated incidental injury or collateral damage must not be excessive in light of the military advantage expected to be gained.

[7] Peter Leahy, "Chief of Army's Address to Land Warfare Conference 2007," public speech, Adelaide Convention Center, Adelaide, Australia, September 24, 2007. Transcript available on line at http://www.defence.gov.au/media/speechtpl.cfm?CurrentId=7208.

[8] Ibid.

[9] Kilcullen, *Out of the Mountains*, 195.

[10] Ibid., 28.

[11] Leahy, "Chief of Army's Address to Land Warfare Conference 2007."

embrace the expanding urban environment and the proliferation of information and communication technologies.

The continued growth of urban environments requires a shift in strategic thinking with regard to the military means used to pursue desired end states. Past discussions have focused primarily on how kinetic force should be applied and generally can be grouped into two approaches: direct and indirect combat. The direct approach seeks to *optimize combat* in urban environments. Applications of technology focused on *improving targeting* and lethality of military forces conducting operations in urban terrain are critical. When optimizing direct combat, forces target only key nodes thereby prompting adversaries to expend defense resources. The indirect approach, in contrast, seeks to minimize if not avoid fighting in the cities altogether. Instead, military forces would secure land, sea, and air approaches to the city while delivering precision strikes on identified targets and resources within the city. Both approaches are flawed. They treat the urban area as little more than a challenging terrain with unique operational constraints. Both approaches tend to largely discount the humans occupying the city and relegate them to two artificially discrete categories: enemies and bystanders. While enemies will surely exist within contested urban environments, viewing non-enemies simply as bystanders is a mistake. In a complex urban environment, the non-committed population represents a form of contested territory. The force that effectively provides the perception of security to the innocent and/or uncommitted population will gain significant advantages, including the ability to maintain force protection, generate actionable intelligence, and leverage essential resources and assets. The force that effectively leverages the population can accomplish this while avoiding catastrophic events that damage credibility and undermine the strategy which brought military forces to the urban area in the first place.[12]

To effectively influence and mobilize contemporary urban populations, a third "combined" approach is required—one that leverages military tools, capabilities resident within other governmental entities and civil society, and information and communication technologies. A combined approach leverages the capabilities of partners with a vested interest in maintaining the stability of the urban area, especially the political entity responsible for the city itself.[13] A combined approach does not discount the use of military force but judiciously applies it proportionately in an effort to minimize negative second order effects. Military Civil Affairs and Military Information Support Forces, moreover, serve as key facilitators and enablers with civilian and civil society partners. This balance requires being prepared to simultaneously identify, seek out, and destroy the enemy while working closely with partners to "protect, support and persuade the population."[14]

Challenges to United States efforts to pursue and protect our national interests are increasingly complex. Preparation for possible conflict with a near peer competitor, such as China, may no longer be the primary concern. While vigilance is always appropriate, current global trends suggest that China—although the *most* likely threat—is, in many ways, the most *un*likely threat. Maintaining control of key populations and domain access points that exist within the boundaries of future urban areas—wherever they are—is essential. Urban environments gain their strategic value from the unique fusion of operational domains. Accounting for this fusion has the potential to yield access across multiple domains and to deliver clear strategic advantage. To ignore or avoid preparing for military operations in massive urban areas is an assured path to operational and strategic failure. The U.S. must pursue strategies to achieve desired ends within massive urban areas and do so without inordinate and unacceptable risks to life, resources, credibility, and political will. In a world where the masses are moving to the city, the U.S. military must be prepared to move there as well.

---

[12] Ibid.
[13] Kilcullen, *Out of the Mountains,* 259.
[14] Leahy, "Chief of Army's Address to Land Warfare Conference 2007."

Army War College Review
Vol. 1, No. 3, Aug. 2015, 41-44

U.S. Army War College
Student Publications

The Rise of China and U.S. Strategy

Derrick Lee

In the wake of two protracted counterinsurgency wars in Iraq and Afghanistan, some would argue that the United States no longer enjoys strong unipolar primacy and that U.S. ability to lead a political, economic and security world order is coming to an end.[1] The primary challenger: China. By virtue of the size of its economy, China is on a trajectory to surpass the U.S. economy, further develop hard- and soft-power influence, and continue to increase military capabilities.[2] Such declinist persuasion, however, may be overly alarmist and pessimistic. On the world stage, the U.S. faces no hegemonic rival. When compared to China over the last decade, the relative strength—both militarily and economically—of the U.S. has risen despite China's impressive growth.[3] The U.S. may yet be able to maintain its position of world leadership, but serious concerns exist. Among them, China's: increasingly hardline and assertive stance, aggressive military actions along claimed borders and spheres of influence, recalcitrance on key global issues, such as free trade, intellectual property, and cyber, and growing revisionist ambition to expand the Chinese role in global affairs and to challenge the current status quo in Asia and the degree of U.S. influence.[4] Despite the need to address a resurgent and revisionist China, current U.S. national security strategy and policies do not provide specific guidelines on how to manage the ever-complex and dynamic relations with revisionist China in the coming decade.

The primary documents[5] guiding U.S. national security and policy offer no comprehensive or detailed outline for how the U.S. will adequately address the risk posed by resurgent China.[6] This

---

Derrick Lee (MSM University of Maryland) is a Lieutenant Colonel in the United States Army. An earlier version of this article was written while the author was a United States Army War College Fellow at Harvard University.

[1] Stephen M. Walt, "The End of the American Era," *National Interest* 116 (November/December 2011): 12.

[2] Arvind Subramanian, "The Inevitable Superpower: Why China's Dominance is a Sure Thing," *Foreign Affairs* 90, no. 5 (September-October 2011)

[3] Michael Beckley, "China's Century? Why America's Edge Will Endure," *International Security* 36, no. 3 (Winter 2011/12): 78.

[4] Walter Russell Mead, "The Return of Geopolitics: The Revenge of the Revisionist Powers," *Foreign Affairs* (May-June 2014), https://www.foreignaffairs.com/articles/china/2014-04-17/return-geopolitics (accessed October 26, 2014).

[5] Five were directly issued by the U.S. government: *National Security Strategy 2010, Quadrennial Defense Review Report 2014, QDR in Perspective Report 2010, Nuclear Posture Review Report 2014, Ballistic Missile Defense Review Report 2010*; two were independent studies sponsored by the U.S. government: *NATO 2020: Assured Security; Dynamic Engagement* (ASDE Report), May 2010 and *Leading Through Civilian Power: The First Quadrennial Diplomacy and Development Review*, December 2010.

[6] Richard L. Kugler, *New Directions in U.S. National Security Strategy, Defense Priorities and Diplomacy* (Washington, DC: National Defense University Press, 2011), vii-viii.

lack of formal guidance with regard to China and the "pivot" to Asia[7] carries both the advantages and disadvantages of ambiguity. The ambiguity of U.S. strategy parallels, in some respects, the generally ambiguous U.S.—China relationship. A certain degree of ambiguity is necessary for dealing with a non-adversarial revisionist power with whom the relationship is not clearly defined. Security strategy or policy predicated on deliberate strategic ambiguity may be effective and warranted in certain discrete situations (as with U.S. policy for cross-strait relations between China and Taiwan).[8] Keeping another global power guessing sans miscalculation, however, creates a delicate balance too subtle to maintain.[9] Strategic ambiguity is simply not a viable long-term strategy for synchronizing elements of national power for effective strategy implementation.

Two decades of unipolar world order in which the United States faced no existential threat or near-peer competitor helped establish the conditions of today's strategic ambiguity. Formulation of a coherent strategy is much easier when presented with a singular, well-defined threat. Panelists at the 2008 U.S. House of Representatives Armed Services Committee Hearing on formulation of a national security priority, for example, testified to the difficulties of formulating a tight, clever, and sophisticated security strategy for the United States due to the lack of an identified existential threat.[10] Because China's revisionism is a recent development, the last two decades have not required concerted U.S. policy and strategy efforts or attention. Successive post-1994 U.S. National Security Strategy documents evidence this. Released by Presidents Clinton, Bush, and Obama, they provide no guidance for truly focusing U.S. national security efforts beyond maintaining and underwriting global security/stability and (post 2001) countering terrorist and violent extremist threat.[11]

Clear priorities must now be established as the U.S. attempts to shift some focus from the Middle East to rebalance security priorities toward Asia.[12] In order to effectively deal with, manage, and if necessary, contain Beijing, U.S. security strategy and policy must be a carefully coordinated and synchronized whole-of-government effort. Washington's official publications outlining U.S. national security strategy, diplomatic efforts, and economic policies must specifically address China's growing revisionist influence and efforts to change the balance of power in the region. Dealing with China should not be a strictly realist strategy aimed at hard-power containment through purely military or security-related endeavors. Rather, U.S. strategy must be predicated on bilateral engagements and multilateral diplomatic efforts to preclude miscalculations or unintended escalation of tensions. But the U.S. must also advance a strategy that establishes clear objectives for maintaining vital U.S. interests in Asia, with requisite security posture and military capacity to hedge against and deter revisionist actions that threaten regional stability.

This task is made more difficult by China's own ambiguity. China is driven by its official foreign policy in which "major powers are the key, surrounding areas are the first priority, developing countries are the foundation, and multilateral forums are the important stage."[13] Yet because China

---

[7] Barack Obama, "Remarks by President Obama to the Australian Parliament," public speech, Parliament House, Canberra, Australia, November 17, 2011.

[8] Pan Zhongi, "U.S. Taiwan Policy of Strategic Ambiguity: A Dilemma of Deterrence," *Journal of Contemporary China* 12, no. 35 (2003): 388.

[9] Ibid., 391.

[10] U.S. Congress, House of Representatives, Committee on Armed Services, Subcommittee on Oversight and Investigations, The New U.S. Grand Strategy, 110th Cong., 2nd sess., July 31, 2008, 2.

[11] Nation Security Strategy of Barack Obama (2010) states that the U.S. will continue to underwrite global security; NSS of George W. Bush (2006, 2002) stresses promotion of democracy and end of tyranny as the main drivers of establishing and maintaining global stability; NSS of William Clinton (2001, 2000, 1998, 1997, 1996, 1995, 1994) promotes engagement with allies and partners and enhancement and employment of U.S. military capability in accordance with the Goldwater-Nichols Act of 1986 to maintain regional and global stability.

[12] Obama, "Remarks by President Obama to the Australian Parliament."

[13] David Shambaugh, "Coping with a Conflicted China," *The Washington Quarterly* 34, no. 1 (Winter 2011): 9.

remains a deeply conflicted rising power, diverse and contradictory actions/positions are often exhibited. Within China tension exists between hard and soft power approaches to national strategy. Under Jiang Zemin and Hu Jintao, China emphasized soft power as the main catalyst for its "peaceful rise" grand strategy.[14] Hard-power realism, however, is gaining ground. For centuries, realism has had a deep-rooted influence in Chinese collective intellectual world view.[15] The notion of hard power realism has been fueled by the growing of China's stature following subjugation and humiliation by colonial powers for much of the past two centuries. Hard power realists advocate the use of China's growing military, economic, and diplomatic influence to coerce others toward the ends China desires, believing that power is worth little if it is not used.[16] Hard power realism driven by narrowly defined self-interests[17] is clearly present in China's foreign policy (e.g., China's increasing aggressiveness towards its neighbors in East and South China Seas, and a series of hardline stances on issues ranging from censorship of Google to declaring restrictive airspace over much of East China Sea). Imbued with a sense of retribution from a long period of China's weakness,[18] hard power realism is advocated by some leading Chinese security experts (e.g., Shen Dingli, the Dean of the School of International Studies at Shanghai's Fudan University) and by some influential policy makers/senior officials of the People's Liberation Army who advocate a strong, forceful response to any encroachment upon China's interests.[19] Beijing has placed great emphasis on modernizing its navy, opaquely increasing defense spending, adopting an anti-access, area defense posture in the Pacific solely aimed at countering U.S. military capability in the region.[20] At the same time, China faces a number of domestic and internal issues that will affect China's outward behavior in an inconsistent and unpredictable manner with significant impact to U.S. interests in the region.[21] These range from a population demographic imbalance, domestic pollution and environmental issues, to an economy that shows signs of plateauing after a decade of growth sustained through extensive exports and manufacturing.[22]

Countering China's seeming hard power initiatives with U.S. hard power may at first seem to be a logical response. Doing so would allow the U.S. to counter Beijing's core interests, including those related to Taiwan, Tibet, Xinjang, and disputed territories in South and East China Seas.[23] A hard power U.S. security strategy would seek to limit China's influence in Asia by (1) establishing a strong military presence in the Pacific, (2) enactly a policy of ''strategic hedging'' with strengthened alliances and partnerships around China's periphery, (3) levying tough economic and trade policies, and (4) leveraging U.S. power and instruments of diplomacy bereft of a concerted engagement effort with China. Hard power alone, however, is ill-advised and should not be the sole, nor even the primary, component of U.S. strategy. At this juncture, China is both a potential adversary and a prospective strategic partner. A hardline hard power U.S. response will exchange ambiguity for adversary, further

---

[14] Xin Li and Verner Worm, *Building China's Soft Power for a Peaceful Rise*, Asian Research Centre, Copenhagen Business School Discussion Paper (Copenhagen: Copenhagen Business School, July 28, 2009): 4.

[15] See Alastair Iain Johnston, *Cultural Realism: Strategic Culture and Grand Strategy in Chinese Culture* (Princeton: Princeton University Press, 1998).

[16] Shambaugh, "Coping with a Conflicted China," 12.

[17] Shambaugh, "Coping with a Conflicted China," 24.

[18] Ibid., 13.

[19] Shen Dingli, "Presentation at the New Zealand Institute of International Affairs," public speech, Victoria University of Wellington, New Zealand, June 28, 2010.

[20] Geoff Dyer, "China vs. U.S.: Is this the New Cold War?" *Financial Times* (February 24, 2014), 1.

[21] Shambaugh, "Coping with a Conflicted China," 25.

[22] Ruchir Sharma, "China's Illusory Growth Numbers," *Dow Jones Wire Chinese (English)*, October 30, 2013.

[23] Wu Xinbo, "China and the United States: Core Interests, Common Interests, and Partnership," *United States Institute of Peace Special Report 277*, June 2011, 1.

entrenching Beijing's rigid obstinacy while increasing tensions and the prospect for escalatory conflict.

The U.S. and, indeed, the world cannot afford the fallout. Rather U.S. strategy and policy efforts with China should be based on cooperation grounded in a position of strength.[24] To be successful, the U.S. must focus on leveraging bilateral relations with its key allies—Japan, South Korea, Australia, Thailand, and Philippines—as a foundation for building a long-term multilateral institution that avoids unnecessarily provoking China while providing incentives rooted in common interests to help elicit Chinese cooperation.[25] Active diplomatic and economic engagement backed by a strong U.S. military posture is required. The U.S. should adopt neither an overly optimistic framework of global cooperation nor an unduly pessimistic relationship of inevitable conflict. A strong, effective U.S. policy toward China will be assertive and prudently realistic, taking every viable measure to avoid military conflict while not shirking from situationally necessary diplomatic confrontation.

[24] Patrick D. Cronin, ed., *Cooperation from Strength: United States, China and the South China Sea* (Washington, DC: Center for New American Security, 2011): 24.

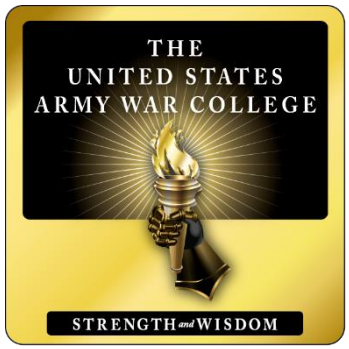
[25] Ibid., 23.

The United States Army War College

The United States Army War College educates and develops leaders for service at the strategic level while advancing knowledge in the global application of Landpower.

The purpose of the United States Army War College is to produce graduates who are skilled critical thinkers and complex problem solvers. Concurrently, it is our duty to the U.S. Army to also act as a "think factory" for commanders and civilian leaders at the strategic level worldwide and routinely engage in discourse and debate concerning the role of ground forces in achieving national security objectives.

SSI STRATEGIC STUDIES INSTITUTE	The Strategic Studies Institute publishes national security and strategic research and analysis to influence policy debate and bridge the gap between military and academia.
CSLD CENTER for STRATEGIC LEADERSHIP and DEVELOPMENT U.S. ARMY WAR COLLEGE	The Center for Strategic Leadership and Development contributes to the education of world class senior leaders, develops expert knowledge, and provides solutions to strategic Army issues affecting the national security community.
PKSOI	The Peacekeeping and Stability Operations Institute provides subject matter expertise, technical review, and writing expertise to agencies that develop stability operations concepts and doctrines.
U.S. Army War College SLDR Senior Leader Development and Resiliency	The Senior Leader Development and Resiliency program supports the United States Army War College's lines of effort to educate strategic leaders and provide well-being education and support by developing self-awareness through leader feedback and leader resiliency.
SCHOOL OF STRATEGIC LANDPOWER U.S. Army War College	The School of Strategic Landpower develops strategic leaders by providing a strong foundation of wisdom grounded in mastery of the profession of arms, and by serving as a crucible for educating future leaders in the analysis, evaluation, and refinement of professional expertise in war, strategy, operations, national security, resource management, and responsible command.
UNITED STATES ARMY HERITAGE AND EDUCATION CENTER	The U.S. Army Heritage and Education Center acquires, conserves, and exhibits historical materials for use to support the U.S. Army, educate an international audience, and honor Soldiers—past and present.


THE
UNITED STATES
ARMY WAR COLLEGE
STRENGTH and WISDOM


U.S.ARMY